UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

JUDITH RAANAN, NATALIE RAANAN, URI RAANAN, R.M., SHAKKED SARAH MATHIAS, SHIR TZIPORAH MATHIAS, ILAN TROEN, RACHEL TROEN, BAR YUVAL SHANI, ERAN SHANI, ARON TROEN, SUSAN TROEN, JUDAH TROEN, HADASSAH TROEN, ABRAHAM TROEN, SANDA MATHIAS, YESHAYAHU MATHIAS, TZAFRIR MATHIAS, REVITAL MATHIAS, MEIRA SEMAMA, AMOS SEMAMA, OREN GLISKO, LIAT RASEL GLISKO, Y.G., ORI GLISKO, VERED BENVENISTE, YOSEF BENVENISTE, CHAYA BENVENISTE, RACHEL OHNONA, JEFFREY LUDMIR, ADI BOSI, DORIAN BOSI, D.B., S.B., H.B., DEBORAH BEN ADERET, YOSEF BEN ADERET, L.B., R.B., and NEVO SHOULIAN, Plaintiffs, -v- BINANCE HOLDINGS LIMITED, and CHANGPENG ZHAO, Defendants.	Case No: 1:24-cv-00697-JGK **AMENDED COMPLAINT**

Plaintiffs Judith Raanan, Natalie Raanan, Uri Raanan, R.M., Shakked Sarah Mathias, Shir Tziporah Mathias, Ilan Troen, Rachel Troen, Bar Yuval Shani, Eran Shani, Aron Troen, Susan Troen, Judah Troen, Hadassah Troen, Abraham Troen, Sanda Mathias, Yeshayahu Mathias, Tzafrir Mathias, Revital Mathias, Meira Semama, Amos Semama, Oren Glisko, Liat Rasel Glisko, Y.G., Ori Glisko, Vered Benveniste, Yosef Benveniste, Chaya Benveniste, Rachel Ohnona, Jeffrey Ludmir, Adi Bosi, Dorian Bosi, D.B, S.B., H.B, Deborah Ben Aderet, L.B., R.B., Yosef Ben Aderet and Nevo Shoulian (collectively, "Plaintiffs"), by their undersigned counsel, as and for their

Complaint against Binance Holdings Limited ("Binance") and Changpeng Zhao ("Zhao"; and together with Binance, "Defendants"), allege as follows:

PRELIMINARY STATEMENT

1. This action is brought by and on behalf of United States citizens who were murdered, maimed, taken hostage, or otherwise injured in unspeakable acts of terrorism perpetrated by Hamas and other terrorist groups in the State of Israel on October 7, 2023. At least thirty United States citizens (including family members of Plaintiffs) were murdered in the attacks, out of a total of approximately 1,200 fatalities. At least ten Americans, including several of the Plaintiffs, were taken hostage in the terrorist attacks that began on October 7, 2023 (the "October 7 Terrorist Attacks"). Hamas and other terrorist groups murdered these victims, filmed their vile acts, and took these hostages in an attempt to extract political concessions from Israel and the United States and inflict terror and pain upon Israeli and United States citizens. Indeed, Plaintiffs continue to suffer traumatic injury as a result of Hamas and Palestinian Islamic Jihad's ("PIJ") ongoing efforts to injure and kill Plaintiffs via further attacks, as well as their publication of death threats and graphic videos of murder and torture of hostages and other victims.

2. By this action, Plaintiffs seek damages under the United States Anti-Terrorism Act ("ATA"), 18 U.S.C. § 2331, *et seq.* from Defendant Binance, a leading cryptocurrency exchange and Defendant Zhao, its founder and former CEO, who for years knowingly provided a mechanism for Hamas and other terrorist groups to raise funds and transact illicit business in support of terrorist activities, which materially contributed to the October 7 Terrorist Attacks, and concealed vital information about this from U.S. regulators and law enforcement.

3. Based on an analysis of Hamas and PIJ wallets using available blockchain data from a leading blockchain analysis firm, Binance processed thousands of transactions valued at

nearly $60 million involving crypto wallets of Hamas and other Palestinian terrorist groups which played a major role in the October 7 Terrorist Attacks. The analysis of the data also showed that Binance processed an additional $42.5 million in transactions involving wallets of Gaza-based money-services businesses. One of these Gaza-based entities has since been designated by the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC") for transmitting money and facilitating transactions for Hamas. Likewise, another was identified by Israel as a "terrorist group" "due to the aid that they provide to the Hamas terrorist organization, particularly its military arm, in transferring funds on a scale of tens of millions of dollars a year." These were direct transactions between Binance and the relevant wallets or were part of multi-step transactions that bear indicia of money laundering. Upon information and belief, there may be many more similar terrorist-related transactions leading up to the October 7 Terrorist Attacks that are known only to Binance and are not yet knowable to the public. No one but Binance has access to Binance's proprietary, non-public transaction data.

4. Binance knowingly provided material support to Hamas, PIJ and other terrorist groups that took part in the October 7 Terror Attacks. Indeed, for years leading up to October 7, 2023, Binance purposely and intentionally built itself up into an illicit financing tool for criminal activity. And Binance intentionally structured its operations to hide this fact from U.S. regulators. Moreover, and since no later than 2019, through evidence presented directly to Binance by governmental entities and its third-party service provider, Binance knew that it been providing services to Hamas, which had been using its exchange to solicit donations, fund itself, and transfer money. Indeed, Hamas publicly admitted well before October 7, 2023 that it was using Binance to fund its activities.

5. Confronted with direct evidence that Hamas, PIJ and other terrorists were using its exchange, Binance filed no required suspicious activity reports ("SARs") with U.S. regulators, did not freeze the terrorists' funds where required by U.S. law, and failed to stop the terrorists from using its platform. It took no meaningful steps to strengthen its internal controls to prevent terrorists from continuing to use its exchange and failed to augment its ability to identify terrorist-related accounts, even though those capabilities existed and were available to Binance. To the contrary, Binance took ***affirmative steps*** to enable users linked to Hamas, PIJ and other terrorist groups to evade regulatory scrutiny. In one instance and as revealed by the United States Department of the Treasury Financial Crimes Enforcement Network ("FinCEN") in its November 2023 consent order against Binance, after a service provider flagged Binance accounts associated with Hamas, Binance's Chief Compliance Officer directed that Binance should "***let him take his funds and leave***," and tipped the terrorists off that the identity of their accounts were known, instructing another employee to *"**Tell him that third party compliance tools flagged him***." (Emphasis added). Binance deliberately hid the truth from U.S. regulators, with FinCEN concluding in its November 2023 consent order that "***Binance senior management misled U.S. authorities***," and "***Binance's willful failure to implement an effective [anti-money laundering] program directly led to the platform being used to process transactions related to . . . terrorist financing***." (Emphasis added).

6. Binance long developed and cultivated a corporate culture of seeing nothing and saying nothing—it knew about criminal activity taking place on its platform while intentionally evading the necessary scrutiny of U.S. regulators. As set forth by the United States Commodity Futures Trading Commission ("CFTC") in a March 2023 civil complaint against Binance and Zhao, Binance's Chief Compliance Officer stated in 2020 that removing accounts associated with

criminal activity from Binance amounted to "offboarding" which was "bad in [Defendant Zhao's] eyes." And this was the name of the game for Binance. As set forth by the CFTC in its complaint against Binance, when subordinates presented Binance's Chief Compliance Officer with evidence that criminals had flocked to the platform he responded with mockery: "***Like come on. They are here for crime***." (Emphasis added). Similarly, as the United States Attorney's Office for the Western District of Washington set forth in its November 2023 criminal complaint against Binance, one Binance compliance officer concluded that Binance was knowingly attracting criminals to its exchange, with the employee writing to other Binance employees that "***we need a banner 'is washing drug money too hard these days - come to binance we got cake for you***.'" (Emphasis added). Indeed, Binance was not only apprised of criminals, including terrorist groups like Hamas and PIJ, transacting on its exchange but internally touted itself as the go-to destination for easy money laundering.

7. That Binance intentionally structured itself as a refuge for illicit activity and knew that terrorists were using its exchange has been borne out in U.S. court filings. Criminal plea agreements and civil settlements that were announced in late 2023 by the U.S. Department of Justice ("DOJ") and various U.S. regulators disclosed that for years Binance and its cofounder and at-the-time Chief Executive Officer, Defendant Zhao, permitted terrorists and illicit actors to transact on Binance's exchange, invited such activity, and intentionally avoided putting into place the legally-mandated infrastructure used to identify, report, and prevent terrorism financing – all in violation of U.S. law. Indeed, for years leading up to the October 7 Terrorist Attacks, Binance's corporate culture was contemptuous of regulatory scrutiny, and internally mocked U.S. regulators' attempts at overseeing its conduct.

8. Defendant Zhao has since been found guilty of various crimes related to Binance's massive, multi-year scheme of evading U.S. regulators. On April 30, 2024, at his sentencing hearing, Zhao addressed his crimes in allowing terror groups to operate unimpeded on Binance by admitting: "I failed to implement an adequate anti-money laundering program ... I realize now the seriousness of that mistake." "I'm sorry," Zhao told the judge before being sentenced. Zhao's belated apology underscores the seriousness of his and Binance's crimes, and the fact that their enabling of Hamas, PIJ and other terrorist groups had consequences. While Zhao was forced to step down as CEO, he retains an overwhelming ownership interest in Binance.

9. As detailed herein, Binance's misconduct substantially assisted the October 7 Terrorist Attacks.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. §§ 2333(a), which provides for jurisdiction over civil actions brought by citizens of the United States, their estates, and family members who have been killed or injured by reason of acts of international terrorism.

11. This Court has personal jurisdiction over Binance under N.Y. § CPLR 302(a) because Plaintiffs' claims against Binance arise from its conduct and operations in New York, including (as described further below) and as set forth in the CFTC complaint as well as by the United States Securities and Exchange Commission ("SEC") in its June 2023 complaint against Binance and Zhao, the fact that several of Binance's key "market makers" were headquartered in and directed trading from New York. These market makers provided critical and deliberately sought-after liquidity to Binance's international exchange, Binance.com, effectively fueling an unregulated marketplace that gave known terrorist groups, including Hamas and PIJ, the ability to

freely trade and transfer cryptocurrency and accept direct donations.

12. Further, as alleged herein, Binance purposefully availed itself of the New York banking system in the course of providing substantial assistance to Hamas and other terrorist groups which played a major role in the October 7 Terrorist Attacks.

13. Further, from September 2019 through February 2023 Binance issued an unregulated security, BUSD, in partnership with Paxos Trust Company ("Paxos"), a New York limited purpose trust company. BUSD is a U.S. dollar-backed stablecoin and those USD reserves were maintained by Paxos in New York. Stablecoins are a type of cryptocurrency that are designed to maintain a constant price in terms of another asset. In November 2021, Binance explained that a "key characteristic of BUSD is that one unit of BUSD is equivalent to one US dollar." Binance added that "BUSD acts as a bridge between traditional finance and [decentralized finance], presenting a newfound level of monetary freedom that isn't offered by traditional currencies or institutions." Stablecoins pegged to USD, such as BUSD and Tether, are more "money-like" than other cryptocurrencies. They can be used to move a derivative of USD across borders without going through regulated U.S. banks that would otherwise monitor this activity. Similarly, stablecoins pegged to USD can be withdrawn into USD. Binance and Paxos also had a profit-sharing agreement to invest those reserves for their mutual benefit. As of February 2023, over $16 billion worth of BUSD were in circulation.

14. Alternatively, this Court may exercise personal jurisdiction over Binance pursuant to FRCP 4(k)(1)-(2).

15. Further, investigations by the DOJ and U.S. regulators found that Binance secretly provided service to millions of users in the United States between August 2017 and October 2022. By September 2020, Binance internal documents attributed 16 percent of its total user base, or

2.51 million users, to the United States, more than any other country. The following month and as the CFTC determined in its March 2023 complaint against Binance and Zhao, Zhao directed Binance personnel to categorize U.S. users as "unknown," for a total of 2.83 million "unknown" customers, or 17 percent of its userbase. According to Binance's own transaction data, U.S. users conducted trillions of dollars in transactions on the platform between August 2017 and October 2022 – transactions that generated over $1.6 billion in profit for Binance. Upon information and belief, many of these U.S. customers and transactions were located in New York. Additionally, a cloud computing platform and application programming service operated by a U.S. technology service provider also hosted Binance's website, stored Binance's data, and operated Binance's exchange.

16. According to Binance's November 2023 settlement agreement with OFAC, "[f]rom approximately August 2017 to October 2022" Binance "matched and executed virtual currency trades on its online exchange platform ***between U.S. person users and users in sanctioned jurisdictions or blocked persons.***" (Emphasis added). Upon information and belief, these included customers located in New York. Pursuant to Binance's settlement with OFAC, these transactions which constituted "direct or indirect exportation or other supply of goods and services ***from the United States***, or ***by U.S. persons***, to users whom [Binance] identified through its Know Your Customer (KYC) process . . . as being [sanctioned entities or in sanctioned jurisdictions] . . . resulted in at least 1,667,153 virtual currency transactions – totaling approximately $706,068,127." (Emphasis added).

17. This Court has personal jurisdiction over Zhao pursuant to N.Y. CPLR § 302(a) as an individual corporate officer who supervised and controlled the activity subjecting Binance to jurisdiction above. *See Chloe v. Queen Bee of Beverly Hills, LLC*, 616 F.3d 158, 163-64 (2d Cir.

2010). This Court also has jurisdiction over Zhao because he conspired with Binance and other agents to conceal their illegal operation of an unlicensed money transmitting business and agents acting at Zhao's direction engaged in overt acts in New York on Zhao and Binance's behalf, including aiding New York-based trading firms in circumventing technological controls in order to supply needed liquidity to Binance's platform. Between 2019 and 2023, Zhao also owned and controlled multiple offshore entities that maintained accounts at Signature Bank in New York and were the counterparties to many large transactions with Binance totaling in the hundreds of millions of dollars. Alternatively, this Court may exercise personal jurisdiction over Zhao pursuant to Rule 4(k)(1)-(2) of the Federal Rules of Civil Procedure

18. Venue is proper in this District pursuant to 18 U.S.C. § 2334(a) and 28 U.S.C. §§ 1391(b), (c)(3), and (d).

THE PARTIES

Plaintiffs

Raanan Family

19. Plaintiff Judith Raanan was taken hostage by Hamas during the terrorist attack committed by Hamas and PIJ at the Kibbutz Nahal Oz in Israel that began on October 7, 2023. At the time of the acts alleged, and at all other times relevant hereto, Judith Raanan was a citizen of the United States. Plaintiff Judith Raanan suffered severe mental anguish and extreme emotional pain and suffering as a result of Hamas's taking her and her daughter (Plaintiff Natalie Raanan) hostage from Kibbutz Nahal Oz, which they were visiting. Hamas terrorists forcibly kidnapped Judith Raanan and physically held her against her will, in fear for her and her daughter's lives. Judith Raanan was released on or about October 20, 2023, after being held captive for approximately two weeks.

20. Plaintiff Natalie Raanan was taken hostage by Hamas during the terrorist attack committed by Hamas and PIJ at the Kibbutz Nahal Oz in Israel that began on October 7, 2023. At the time of the acts alleged, and at all other times relevant hereto, Natalie Raanan was a citizen of the United States and the daughter of Plaintiff Judith Raanan. At the time she was taken hostage, Natalie Raanan was a minor child. Plaintiff Natalie Raanan suffered severe mental anguish and extreme emotional pain and suffering as a result of Hamas's taking her and her mother hostage. Hamas terrorists forcibly kidnapped Natalie Raanan and physically held her against her will, in fear for her and her mother's lives. Natalie Raanan was released on or about October 20, 2023, after being held captive for approximately two weeks.

21. Plaintiff Uri Raanan is the father of plaintiff Natalie Raanan and ex-husband of plaintiff Judith Raanan. Plaintiff Uri Raanan suffered severe mental anguish and extreme emotional pain and suffering as a result of the fact that Natalie and Judith Raanan were attacked by Hamas and PIJ and then taken hostage in the October 7, 2023 terrorist attack.

Matthias Family

22. Shachar Deborah Troen Mathias ("Shachar") and her husband Shlomi David Mathias ("Shlomi") were killed by Hamas in their home during the October 7 terrorist attacks by Hamas and PIJ in Kibbutz Holit, a small village in Israel. At the time of the acts alleged, and at all other times relevant hereto, Shachar was a citizen of the United States.

23. Plaintiff R.M., aged sixteen, woke up at around 6:30 am on October 7, 2023, in his parents' home on Kibbutz Holit to rockets being launched from Gaza during the Hamas and PIJ joint attack. R.M.'s parents, Shachar and Shlomi, ushered R.M. into their home's bomb shelter. Different from a panic room, their bomb shelter is designed to be accessible from the outside. Kibbutz Holit then issued an infiltration message that terrorists had infiltrated the village.

Simultaneously, Shachar and Sholmi told their two daughters to shelter in place – they had been sleeping at two different homes in the village. R.M., Shachar and Shlomi then heard automatic weapons, grenades, rocket propelled grenades, and yelling. Soon after, R.M., Shachar and Shlomi heard glass shattering in their home. Shlomi then directed R.M. to barricade the shelter and then hide under a mattress. Shachar then laid on top of R.M. further shielding him.

24. The terrorists approached the bomb shelter, yelled "Allahu Akbar", then entered the shelter room, threw a grenade, and sprayed the room with bullets. Shachar was killed instantly while on top of R.M. – protecting her son with her body. Shlomi had tried to fight the terrorists out of the room and yelled his arm had been blown off, and watched his wife die before dying from his own wounds. R.M. felt heat in his stomach and a strange taste in his mouth. R.M. opened his extended family group WhatsApp chat and typed that his parents were dead. In shock and horror, his family thought he was joking or exaggerating. At that point, R.M. noticed a bullet wound in his abdomen (that had travelled through his mother's body) and subsequently discovered shrapnel from the grenade in his eyelid and ankle. R.M. continued to wait about 45 minutes under his mother's lifeless body until he felt compelled to move because there was so much smoke, and breathing was too difficult.

25. Upon getting up from under the mattress and his mother's body, R.M. saw clumps of his parents' human remains on himself, the bed, and the walls. R.M. then came to believe that the taste in his mouth was likely his parents' remains. R.M. then exited the home to hide in an exterior room of the home where he continued to hear and see the massacre of his neighbors and friends. Once the smoke lessened from inside the home, R.M. reentered the home and found that it was black from soot. He took a glance into the shelter and saw his father's dead body. As R.M. heard the terrorists coming back, he hid in his parents' room in terror for hours. The Israeli army

eventually evacuated R.M. from the home. As he was being evacuated, R.M witnessed the carnage on the way to the hospital where he also witnessed the massacre including gruesome dead bodies, scenes of destruction, and wounded people holding their own severed limbs. Plaintiff R.M. suffered physical injuries, severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack that claimed the life of his parents. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff R.M. was a citizen of the United States.

26. Plaintiff Shakked Sarah Mathias is the daughter of Shachar and Shlomi who were killed by Hamas in their home during the October 7 terrorist attacks by Hamas and PIJ on Kibbutz Holit, a small village in Israel. Plaintiff Shakked Sarah Mathias' first communication from her parents and brother when the attack began was a WhatsApp notification from R.M. that her parents were killed. Her phone then lost service for approximately the next fourteen hours, leaving R.M. and the rest of the Mathias extended family to presume she had been killed in Kibbutz Holit where she was also staying. Plaintiff Shakked Sarah Mathias, alone in terror, heard the terrorist attacks throughout the day, including armed terrorists loitering outside her window. Plaintiff Shakked Sarah Mathias suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack that claimed the life of her parents. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Shakked Sarah Mathias was a citizen of the United States.

27. Plaintiff Shir Tziporah Mathias is the daughter of Shachar and Shlomi who were killed by Hamas in their home during the October 7 terrorist attacks by Hamas and PIJ on Kibbutz Holit, a small village in Israel. Plaintiff Shir Tziporah Mathias' first communication from her parents and brother when the attack began was a WhatsApp notification from R.M. that her parents were killed. Her phone then lost service for approximately the next fourteen hours leaving R.M.

and the rest of the Mathias extended family to presume she had been killed in Kibbutz Holit where she was also staying. Plaintiff Shir Tziporah Mathias, alone in terror, heard the terrorist attacks throughout the day, including armed terrorists loitering outside her window. At one point the terrorists entered her apartment but did not see her in her hiding place. Plaintiff Shir Tziporah Mathias suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack that claimed the life of her parents. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Shir Tziporah Mathias was a citizen of the United States.

28. Plaintiff Ilan Troen is the father of Shachar, father in-law of Shlomi and grandfather to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Ilan Troen was traumatized from witnessing the attack by Hamas and PIJ terrorists unfold, receiving the news of the murders over WhatsApp of Shachar and Shlomi, losing contact with Shakked and Shir whom he feared were murdered, and following R.M.'s terror, all while powerless to help. And he witnessed all this from his own bomb shelter with rocket attacks over his home. Plaintiff Ilan Troen suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Ilan Troen was a citizen of the United States.

29. Plaintiff Rachel Troen is the mother of Shachar, mother in-law of Shlomi and grandmother to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Rachel Troen was traumatized from witnessing the attack by Hamas and PIJ terrorists unfold, receiving the news of the murders over WhatsApp of Shachar and Shlomi, losing contact with Shakked and Shir whom she feared were murdered, and following R.M.'s terror, all while

powerless to help. And she witnessed all this from her own bomb shelter with rocket attacks over her home. Plaintiff Rachel Troen suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Rachel Troen was a citizen of the United States.

30. Plaintiff Bar Yuval Shani is the sister of Shachar, sister in-law of Shlomi and aunt to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Bar Yuval Shani was traumatized from witnessing the attack by Hamas and PIJ terrorists unfold, receiving the news of the murders over WhatsApp of Shachar and Shlomi, losing contact with Shakked and Shir whom she feared were murdered, and following R.M.'s terror, all while powerless to help. And she witnessed all this from her own bomb shelter with rocket attacks over her home. Plaintiff Bar Yuval Shani suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Bar Yuval Shani was a citizen of the United States.

31. Plaintiff Eran Shani, an Israeli citizen, is the brother-in-law of Shachar and Shlomi and uncle to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Eran Shani was traumatized from witnessing the attack by Hamas and PIJ terrorists unfold, receiving the news of the murders over WhatsApp of Shachar and Shlomi, losing contact with Shakked and Shir whom he feared were murdered, and following R.M.'s terror, all while powerless to help. And he witnessed all this from his own bomb shelter with rocket attacks over his home. Plaintiff Eran Shani suffered severe mental anguish and extreme emotional pain and suffering as a result of the

October 7, 2023 terrorist attack that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias.

32. Plaintiff Aron Troen is the brother of Shachar, brother in-law of Shlomi and uncle to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Aron Troen was traumatized from witnessing the attack by Hamas and PIJ terrorists unfold, receiving the news of the murders over WhatsApp of Shachar and Shlomi, losing contact with Shakked and Shir whom he feared were murdered, and following R.M.'s terror, all while powerless to help. And he witnesses all this from his own bomb shelter with rocket attacks over his home. Plaintiff Aron Troen suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Aron Troen has also become the legal guardian and foster parent to Plaintiff R.M as a result of the October 7, 2023 terrorist attack that killed R.M.'s parents. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Aron Troen was a citizen of the United States. Plaintiff Aron Troen brings this action individually and on behalf Plaintiff R.M. who is a minor.

33. Plaintiff Susan Troen is the sister-in-law of Shachar and Shlomi and aunt to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Susan Troen was traumatized from witnessing the attack by Hamas and PIJ terrorists unfold, receiving the news of the murders over WhatsApp of Shachar and Shlomi, losing contact with Shakked and Shir whom she feared were murdered, and following R.M.'s terror, all while powerless to help. And she witnessed all this from her own bomb shelter with rocket attacks over her home. Plaintiff Susan Troen suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack that claimed the life of Shachar and Shlomi and injured Plaintiffs

R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Susan Troen has also become the legal guardian and foster parent to Plaintiff R.M as a result of the October 7, 2023 terrorist attack that killed R.M.'s parents. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Susan Troen was a citizen of the United States.

34. Plaintiff Judah Troen is the brother of Shachar, brother in-law of Shlomi and uncle to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Judah Troen was traumatized from witnessing the attack by Hamas and PIJ terrorists unfold, receiving the news of the murders over WhatsApp of Shachar and Shlomi, losing contact with Shakked and Shir whom he feared were murdered, and following R.M.'s terror, all while powerless to help. And he witnessed all this from his own bomb shelter with rocket attacks over his home. Plaintiff Judah Troen suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Judah Troen was a citizen of the United States.

35. Plaintiff Hadassah Troen is the sister-in-law of Shachar and Shlomi and aunt to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Hadassah Troen was traumatized from witnessing the attack by Hamas and PIJ terrorists unfold, receiving the news of the murders over WhatsApp of Shachar and Shlomi, losing contact with Shakked and Shir whom she feared were murdered, and following R.M.'s terror, all while powerless to help. And she witnessed all this from her own bomb shelter with rocket attacks over her home. Plaintiff Hadassah Troen suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. At the time of the acts alleged, and at

all other times relevant hereto, Plaintiff Hadassah Troen was a citizen of the United States.

36. Plaintiff Abraham Troen is the brother of Shachar, brother in-law of Shlomi and uncle to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Abraham Troen was traumatized from witnessing the attack by Hamas and PIJ terrorists unfold, receiving the news of the murders over WhatsApp of Shachar and Shlomi, losing contact with Shakked and Shir whom he feared were murdered, and following R.M.'s terror, all while powerless to help. Plaintiff Abraham Troen suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Abraham Troen was a citizen of the United States.

37. Plaintiff Sanda Mathias, an Israeli citizen, is the mother in-law of Shachar, mother of Shlomi and grandmother to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Sanda Mathias suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias.

38. Plaintiff Yeshayahu Mathias, an Israeli citizen, is the father in-law of Shachar, father of Shlomi and grandfather to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Yeshayahu Mathias suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias.

39. Plaintiff Tzafrir Mathias, an Israeli citizen, is the brother in-law of Shachar, brother of Shlomi and uncle to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Tzafrir Mathias suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias.

40. Plaintiff Revital Mathias, an Israeli citizen, is the sister in-law of Shachar, sister in-law of Shlomi and aunt to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Revital Mathias suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias.

41. Plaintiff Meira Semama, an Israeli citizen, is the sister in-law of Shachar, sister of Shlomi and aunt to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Meira Semama suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias.

42. Plaintiff Amos Semama, an Israeli citizen, is the brother in-law of Shachar, brother in-law of Shlomi and uncle to Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias. Plaintiff Amos Semama suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ that claimed the life of Shachar and Shlomi and injured Plaintiffs R.M., Shakked Sarah Mathias, and Shir Tziporah Mathias.

Glisko Family

43. Itay Glisko was murdered at the age of twenty during the terrorist attack that began on October 7, 2023. At 11 a.m. on October 7, 2023, Itay Glisko reached out to his family to tell

them that his Israeli army base had been invaded by Hamas and PIJ in a surprise attack, and that he was not sure if this was the last time he would speak to them. In his last texts to his family, Itay Glisko also stated that his friends had been shot and that he was helping the injured. He wrote to his brother that he was afraid but would fight like a hero. At the time of the acts alleged, and at all other times relevant hereto, Itay Glisko was a citizen of the United States.

44. Plaintiff Oren Glisko, an Israeli citizen, is the father of United States citizen Itay Glisko. Plaintiff Oren Glisko suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ that claimed the life of Itay Glisko. Plaintiff Oren Glisko brings this action individually and on behalf of Plaintiff Oren Glisko's minor child, Y.G.

45. Plaintiff Liat Rasel Glisko, an Israeli citizen, is the mother of United States citizen Itay Glisko. Plaintiff Liat Rasel Glisko has suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ that claimed the life of her son Itay Glisko.

46. Plaintiff Y.G. is a minor child, an Israeli citizen, and the brother of United States citizen Itay Glisko. Plaintiff Y.G. suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ that claimed the life of his brother, Itay Glisko.

47. Plaintiff Ori Glisko, an Israeli citizen, is the brother of United States citizen Itay Glisko. Plaintiff Ori Glisko suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ that claimed the life of his brother, Itay Glisko.

Benveniste Family

48. Arnon Benveniste was murdered at the age of twenty-six by Hamas in November 2023 while serving in the Israel Defense Forces ("IDF"), fighting Hamas and PIJ in Gaza. Arnon Benveniste's grandfather was killed in the Yom Kippur War and his uncle and namesake was killed in the Lebanon war. At the time of the acts alleged, and at all other times relevant hereto, Arnon Benveniste was a citizen of the United States.

49. Plaintiff Vered Benveniste is the mother of Arnon Benveniste. Plaintiff Vered Benveniste suffered severe mental anguish and extreme emotional pain and suffering as a result of the Hamas attack that claimed the life of her son, Arnon Benveniste. At the time of the acts alleged, and at all other times relevant hereto, Vered Benveniste was a citizen of the United States.

50. Plaintiff Yosef Benveniste is the brother of Arnon Benveniste. Plaintiff Yosef Benveniste suffered severe mental anguish and extreme emotional pain and suffering as a result of the Hamas attack that claimed the life of his brother, Arnon Benveniste. At the time of the acts alleged, and at all other times relevant hereto, Yosef Benveniste was a citizen of the United States.

51. Plaintiff Chaya Benveniste is the twin sister Arnon Benveniste. Plaintiff Chaya Benveniste suffered severe mental anguish and extreme emotional pain and suffering as a result of the Hamas attack that claimed the life of her brother, Arnon Benveniste. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Chaya Benveniste was a citizen of the United States.

Rachel Ohnona

52. Plaintiff Rachel Ohnona is the mother of Alexandre Look who was murdered at the age of 33 at the Supernova Peace Festival during the October 7, 2023, terrorist attacks by Hamas and PIJ. Alexandre Look was hiding inside a bomb shelter that did not have a door. In a heroic

final deed, Alexandre Look fought off terrorists with his bare hands, acting as the barrier between them and the approximately 25 other people inside the bunker where he was sheltering. Plaintiff Rachel Ohnona suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023, terrorist attack by Hamas and PIJ that claimed the life of her son. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Rachel Ohnona was a citizen of the United States.

Jeffrey Ludmir

53. Plaintiff Jeffrey Ludmir is a U.S. citizen residing in Miami, Florida. Mr. Ludmir is the uncle of Dr. Daniel Levi Ludmir, a native of Peru and a physician at the Soroka Medical Center in Beersheba, Israel, who was murdered during the joint Hamas and PIJ terrorist attack while treating the wounded at Kibbutz Be'eri on October 7, 2023. Jeffrey Ludmir suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ that claimed the life of his nephew Daniel Levi.

54. When Daniel Levi was a young boy, his father abandoned his mother and siblings. With Daniel Levi's father being absent for over 25 years, Jeffrey Ludmir assumed the role of a father figure for his nephew, Daniel Levi. Mr. Ludmir played a guardian-like role in providing monetary support to his sister (Daniel Levi's mother) to help her raise Daniel Levi and her other two children. He would often speak with Daniel Levi on the phone and would visit him in Peru where he was born and raised. Daniel Levi also traveled to Miami repeatedly in order to visit Jeffrey Ludmir in Miami.

Bosi Family

55. Plaintiff Adi Bosi was pregnant on October 7, 2023, when her city, Sderot, was attacked by Hamas and PIJ. On the morning of October 7, 2023, the Bosi family was having

breakfast when they heard a sound like thunder. From the sixth floor of her apartment, Adi Bosi saw vehicles on the streets and people being shot at. Adi Bosi and her family escaped to their bomb shelter before gunfire hit their home. For about twenty hours Adi Bosi hid in a shelter with her toddlers, D.B. aged three, S.B. aged two, and her husband as they heard rockets and missiles landing and the sound of bullets throughout the streets and feared for their lives. Adi Bosi suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ. At the time of the acts alleged, and at all other times relevant hereto, Adi Bosi was a citizen of the United States. Plaintiff Adi Bosi brings this action individually and on behalf of her minor children, Plaintiffs D.B., S.B., and H.B.

56. Plaintiff Dorian Bosi, an Israeli citizen, is the husband of United States citizen Adi Bosi. Plaintiff Dorian Bosi suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023, terrorist attack by Hamas and PIJ.

57. Plaintiff D.B. is a minor child and the son of United States citizen Adi Bosi. Plaintiff D.B. suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff D.B. was a citizen of the United States.

58. Plaintiff S.B. is a minor child and the daughter of United States citizen Adi Bosi. Plaintiff S.B. suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff S.B. was a citizen of the United States.

59. Plaintiff H.B. is a minor child and the daughter of United States citizen Adi Bosi. Plaintiff H.B. was born to Adi Bosi after the attack and suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023 terrorist attack by Hamas and PIJ

due to the deep impact on her family. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff H.B. was a citizen of the United States.

Ben Aderet Family

60. Plaintiff Deborah Ben Aderet along with her two minor children, L.B. aged six, R.B. aged eight, and her husband Yosef Ben Aderet hid in their shelter in Zikim beginning early on October 7, 2023, when they heard the attack by Hamas and PIJ begin. Fearing for their lives and without any means of self-defense, Plaintiff Deborah Ben Aderet and her husband Yosef Ben Aderet armed themselves with kitchen knives. The family heard the attacks until they were evacuated the next day by the IDF. Upon their evacuation the family passed dead bodies in the streets. At the time of the acts alleged, and at all other times relevant hereto, Deborah Ben Aderet was a citizen of the United States. Plaintiff Deborah Ben Aderet brings this action individually and on behalf of her minor children, Plaintiffs L.B., and R.B.

61. Plaintiff Yosef Ben Aderet, an Israeli citizen, is the husband of United States citizen Deborah Ben Aderet. Plaintiff Dorian Bosi suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023, terrorist attack by Hamas and PIJ.

62. Plaintiff L.B. is a minor child and the son of United States citizen Deborah Ben Aderet. Plaintiff L.B. suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023, terrorist attack by Hamas and PIJ. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff L.B. was a citizen of the United States.

63. Plaintiff R.B. is a minor child and the son of United States citizen Deborah Ben Aderet. Plaintiff R.B. suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023, terrorist attack by Hamas and PIJ. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff R.B. was a citizen of the United States.

Nevo Shoulian

64. On October 7, 2023, Plaintiff Nevo Shoulian was at the Supernova Peace Festival when Hamas and PIJ terrorists attacked. Although Nevo Shoulian survived, he witnessed the attack, assault, murder of his friends who were attending the festival with him. Plaintiff Nevo Shoulian's friends were also kidnapped from the festival. Plaintiff Nevo Shoulian suffered severe mental anguish and extreme emotional pain and suffering as a result of the October 7, 2023, terrorist attack by Hamas and PIJ. At the time of the acts alleged, and at all other times relevant hereto, Plaintiff Nevo Shoulian was a citizen of the United States.

DEFENDANTS

Binance

65. Binance Holdings Limited ("Binance") is an entity registered in the Cayman Islands that holds employment contracts for certain employees operating Binance.com. Binance has stated that it does not have a corporate headquarters and refuses to disclose the location of its main Binance.com exchange.

66. Since at least July 2017, Binance has operated a web-based virtual currency exchange under the name Binance.com that offers trading in virtual currencies, digital asset commodities and related derivatives, among other financial products and services, to over 100 million customers throughout the world.

67. On November 21, 2023, Binance pled guilty to federal charges of failing to maintain an effective anti-money laundering program and entered into settlements with three U.S. regulators in connection with charges of violations of the Bank Secrecy Act and U.S. sanctions. These violations included processing and failing to report transactions—that Binance senior executives had knowledge of—with cryptocurrency wallets linked to terrorist groups such as

Hamas or PIJ, both of which the United States government has since 1997 designated as a foreign terrorist organization ("FTO").

68. Notwithstanding Binance's representations as to its purported lack of business location, at all relevant times, Binance had extensive ties to New York. As detailed further below, many of Binance's "VIP" users were located in New York. For example and as determined by the SEC in its June 2023 complaint against Binance and Zhao, at least two of Binance's VIP "market maker" customers were quantitative trading firms headquartered in New York, one of which, as concluded by the CFTC in its March 2023 complaint against Binance, was "among Binance's largest customers." One of these New York firms conducted trading on Binance's platform through at least 15 independent trading teams. Upon information and belief, other New York-based VIP customers secretly acted as market makers and provided necessary liquidity to the Binance.com platform, effectively fueling an unregulated marketplace that (as described further below) gave known terrorists, including Hamas, PIJ and entities linked to those FTOs, the ability to freely trade cryptocurrency and accept direct donations.

69. As the CFTC detailed in a December 2023 consent order against Binance and Zhao in the Northern District of Illinois, Binance's largest and most important users has included three trading firms headquartered or otherwise based in New York:

Trading Firm A:

- Trading Firm A is a quantitative trading firm that has traded bitcoin perpetuals on Binance, among other products, through at least three different accounts during the Relevant Period. Trading Firm A is a Delaware limited liability company headquartered in Chicago, Illinois. Trading Firm A has offices in New York.

Trading Firm B:

- Trading Firm B is a quantitative trading firm headquartered in New York and incorporated in Delaware. Trading Firm B has at all relevant times been ultimately majority-owned by U.S. residents. Numerous senior managers, including the individual who functions as Trading Firm B's CEO, have worked from Trading Firm B's New York headquarters.

- Trading Firm B conducts its digital asset trading activity on Binance through a dedicated trading desk that utilizes automated trading strategies programmed into computer algorithms developed by personnel at Trading Firm B's New York headquarters. Trading Firm B's algorithms determine whether to place or cancel any orders based on the instructions in their code. Trading Firm B's algorithms are built using computer code that Trading Firm B considers to be valuable intellectual property. Trading Firm B's computer code is owned, directly or by assignment from its various wholly-owned subsidiaries, by Trading Firm B.

- The global head of Trading Firm B's digital asset trading desk works from Trading Firm B's New York headquarters. Other employees, including members of the business development team responsible for interacting with Binance, also work from Trading Firm B's New York headquarters.

- Trading Firm B has been among Binance's largest customers and has consistently received reduced trading fees due to its status as a Binance VIP.

Trading Firm C:

- Trading Firm C, another quantitative trading firm that trades digital asset derivatives on Binance through automated trading strategies, is headquartered and incorporated in New York. Trading Firm C is majority-owned by U.S. residents and the individual with the largest ownership share is also a U.S. citizen. Trading Firm C trades in numerous financial markets around the globe and is part of a corporate "umbrella" of commonly controlled affiliates and subsidiaries that has branch offices in London, Singapore, and Hong Kong, among other locations.

- Zhao communicated directly with Trading Firm C's CEO, who has a New York phone number.

70. Additionally, Binance used accounts at the now-defunct, New York-based Signature Bank to transfer billions of dollars between 2019 and 2022. Headquartered in New York,

Signature Bank had approximately 40 branches in the United States and just under $100 billion in assets before its collapse in 2023.

71. In addition to the accounts held at New York-based Signature Bank on behalf of Binance and other Binance affiliates that were all beneficially owned by Zhao, Zhao also owned and controlled multiple foreign entities that also maintained accounts at Signature Bank and were the counterparties for many of the large transfers described above, totaling hundreds of millions of dollars.

72. In addition, as set forth by the SEC in its June 2023 complaint against Binance, Binance also relied on other New York-based entities to conduct business. For example, Binance relied on Paxos, a New York limited purpose trust company. Beginning in September 2019, pursuant to a "Stablecoin as a Service" agreement with a Binance affiliate, Paxos issued in partnership with Binance a proprietary USD-backed stablecoin called "BUSD," which was approved by and under the supervision of the New York State Department of Financial Services ("NYDFS") but was never registered with the SEC. Binance and Paxos also had a profit-sharing agreement to invest those reserves for their mutual benefit. As of February 2023, over $16 billion worth of BUSD were in circulation.

73. BUSD could be and was traded on the Binance platform until February 2023, when, as the SEC concluded in its June 2023 complaint against Binance, NYDFS ordered Paxos to cease minting BUSD "as a result of several unresolved issues related to Paxos' oversight of its relationship with Binance in regard to Paxos-issued BUSD."

Changpeng Zhao

74. Zhao is Binance's primary founder, majority owner, and was formerly Binance's Chief Executive Officer. He is a Canadian citizen, and, upon information and belief, is a resident

of the United Arab Emirates. Zhao launched Binance in 2017. Together with a core senior management group, as Binance's CEO, Zhao made strategic decisions for Binance, and supervised and exercised day-to-day control over its operations and finances.

75. On November 21, 2023, Zhao pled guilty to willful violations of the Bank Secrecy Act. He agreed to pay a $150 million fine and was sentenced to four months in prison on April 30, 2024. Zhao was also a named party with "control person" liability in regulatory settlements with Binance. On April 30, 2024, at his sentencing hearing, Zhao projected remorse regarding the results of his crimes, stating that he, "realize[s] now the seriousness of that mistake." "I'm sorry," Zhao told the judge before being sentenced. Indeed, those crimes had serious consequences. As further detailed herein, Zhao and Binance provided material support to the terror groups that wrought death and destruction in the October 7 Terrorist Attacks.

FACTUAL ALLEGATIONS

The Hamas Terrorist Organization

76. Hamas emerged in 1987 during the first Palestinian uprising (or intifada) as an outgrowth of the Muslim Brotherhood's Palestinian branch. The group is committed to the destruction of the State of Israel and has launched countless terrorist attacks to destabilize it. Hamas's charter calls for establishing an Islamic Palestinian state in Israel's place. In its pursuit of these goals, Hamas has killed dozens of Americans over the course of decades. These terrorist attacks included an unprecedented wave of suicide bombings during the Second Intifada, from roughly 2000-05, which captured the world's attention and horror due to their barbarity and unusual nature at the time.

77. Hamas has been the *de facto* governing body in the Gaza Strip since June 2007, when it ejected the Palestinian Authority from power in a murderous *coup d'etat* in which over 150 Palestinians died by execution or other means (including by being thrown from rooftops).

According to a 2008 report by Human Rights Watch, during their violent takeover of Gaza, "Hamas forces committed serious violations of international humanitarian and human rights law, including summary executions and torture."

78. Governing responsibilities did not distract Hamas from its primary mission, launching terrorist attacks: notorious periods of Hamas terrorist attacks occurred from 2005-09, 2012, 2014, 2015, 2021, among other periods. Hamas operates primarily in and from Gaza. It also maintains a presence in the West Bank, Palestinian refugee camps in Lebanon, and in Middle Eastern countries, including Iran, Syria, Qatar, and Egypt. Part of Hamas's terrorist campaign against Israel and the United States includes the killing of American citizens who live in or visit Israel.

79. Hamas has a "military wing" known as the Izz al-Din al-Qassam Brigades ("al-Qassam Brigades") that has conducted numerous terrorist attacks in both Israel and the Palestinian territories since the 1990s. The al-Qassam Brigades has been separately and explicitly designated as a terrorist organization by the European Union, Australia, New Zealand, Egypt, and the United Kingdom.

80. The U.S. State Department sanctioned Hamas in 1995 and designated it as a Foreign Terrorist Organization ("FTO") in October 1997. In the decades since, the U.S. has imposed additional sanctions on Hamas's leaders, charities, companies, and facilitators as well as banks acting as financial arms of Hamas.

81. On October 8, 1997, by publication in the Federal Register, the United States Secretary of State designated Hamas an FTO pursuant to Section 219 of the Immigration and Nationality Act and the Antiterrorism and Effective Death Penalty Act of 1996. The designation

of Hamas as an FTO has been renewed every two years since 1997. In 2001, the U.S. Government designated Hamas as a Specially Designated Global Terrorist ("SDGT").

The Palestinian Islamic Jihad Terrorist Organization

82. Palestinian Islamic Jihad ("PIJ") was founded in 1981 as an offshoot of the Muslim Brotherhood in Egypt by Dr. Fathi Ibrahim Abdulaziz Shaqaqi, who was heavily inspired by the Iranian Islamic Revolution. PIJ launched its first attacks on Israeli targets in Gaza in 1984, and, by the late 1980s, its leadership, including Shaqaqi, had been deported to Lebanon, after which Shaqaqi traveled to Tehran where he was promised support by Ayatollah Khomeini. In the late 1980s, PIJ deportees were trained by the IRGC at Hezbollah camps in Lebanon and conducted joint attacks on Israeli forces with Hezbollah. In 1989 PIJ moved its headquarters to Damascus, Syria but maintained a substantial force in Lebanon.

83. In 1992 PIJ established its formal military wing, the Quds Brigades. PIJ opposed the Oslo Accords between Israel and the PLO, and, throughout the 1990s, PIJ carried out attacks in Israel in an attempt to undermine the peace process. During the Second Intifada, PIJ carried out suicide bombings, car bombings, and mass killings on Israeli military and civilian targets. Today, the U.S. State Department estimates that PIJ's membership to be as high as several thousand, making it the second largest terror organization in the Gaza Strip and West Bank.

84. Since as late as 2018, PIJ has coordinated its attacks on Israel with Hamas and other militant groups through an umbrella organization in Gaza known as the "joint operations room." While Hamas and PIJ cooperate in their shared goal of destroying Israel, PIJ is consistently more extremist in ideology and tactics than Hamas, focusing exclusively on violent confrontations with Israel.

85. According to the U.S. State Department's 2021 Country Reports on Terrorism, "PIJ is committed to the destruction of Israel and to the creation of an Islamic state in historic Palestine, including present-day Israel." Accordingly, the U.S. State Department designated PIJ as a FTO in October 1997 and has subsequently designated numerous PIJ supporters and leaders, including designating PIJ's Secretary General Ziyad al-Nakhalah as a SDGT in 2014. In 2001, the U.S. Government designated PIJ as a SDGT.

Relevant Non-Party: The Islamic Republic of Iran

86. The Islamic Republic of Iran ("Iran"), through its political subdivisions, agencies, and instrumentalities, provided Hamas and PIJ with material support and resources that enabled, facilitated and caused the October 7 Terrorist Attacks.

87. Since 1984, Iran has been continuously designated as a state sponsor of terrorism by the U.S. government. The United States State Department's *Country Reports on Terrorism* for 2022 noted that Iran is "the leading state sponsor of terrorism, facilitating a wide range of terrorist and other illicit activities around the world."

Relevant Non-Party: The Syrian Arab Republic

88. The Syrian Arab Republic ("Syria"), through its political subdivisions, agencies, and instrumentalities, provided Hamas and PIJ with material support and resources that enabled, facilitated, and caused the October 7 Terrorist Attacks.

89. Since 1979, Syria has been continuously designated as a state sponsor of terrorism by the U.S. government.

The October 7 Terrorist Attacks

90. On October 7, 2023, several thousand Hamas and PIJ terrorists from Gaza invaded Israel and butchered approximately 1,200 people, many of whom were burned alive or subject to horrific tortures, rapes, mutilations, and other atrocities. Over 350 people were massacred at a

music festival located near Kibbutz Re'im near the Gaza border. Hundreds of others were murdered in communities in southern Israel near the Gaza border. Inevitably and by design, the victims included many Americans.

91. Terrorists from Hamas and PIJ also kidnapped several hundred men, women, and children from Israel and forcibly took them as hostages to Gaza, where many of them were tortured and imprisoned in horrific conditions in poorly ventilated underground tunnels.

92. While the October 7 Terrorist Attacks were planned and led by Hamas, other Palestinian terror groups also participated in the attacks, including PIJ. Several of these terror groups, including Hamas and PIJ, claimed to have captured and held hostages in connection with the attacks.

93. On the day of the attacks or shortly thereafter, Hamas and PIJ broadcast their role in the attacks on English and Arabic language social media. These perverse claims of "ownership" of individual attack on different kibbutz and locations leave no doubt as to the two groups' responsibility for the injuries suffered by the Plaintiffs.

94. For example, on October 7, 2023, the Resistance News Network (a Telegram channel that publishes English translations of propaganda from terrorist groups including Hamas and PIJ) released a video purporting to show armed Hamas terrorists in Sderot, Israel, with the caption "a fierce battle is ongoing in the Zionist settlement of 'Sderot' where al-Qassam fighters are going building-to-building, liberating the land." On October 7, 2023, the PIJ Telegram account Saraya Pulse posted about the attack on Kibbutz Be'eri, announcing the purported "Fall of Kibbutz Bayeri at the hands of the Mujahideen of the Brigades and the Resistance." On the same day, Saraya Pulse also issued a post regarding PIJ's involvement in the terror attacks at Kibbutz Nahal

Oz, stating, "The Mujahideen of Al-Saraya control a Merkava tank and a number of vehicles in the Nahal Al-Oz site…#Al-Aqsa_Flood."

95. The Resistance News Network posted a statement from the Al-Qassam Brigades on October 7, 2023 that the Al-Qassam Brigades were "engaged in fierce confrontations in 'Be'eri'." On the same day, the Resistance News Network posted a video from the Al-Qassam Brigades, captioned "New scenes of the seizure of the 'Nahal Oz' base east of Gaza during the Al-Aqsa Flood Battle."

96. On October 7, 2023, Hamas's Al-Qassam Brigades claimed responsibility for the October 7, 2023 attack on Kibbutz Holit, posting on its Telegram channel that "Clashes continue between the Al-Qassam Mujahideen and the occupation forces in several areas, including: the "Sufa" site and the "Holeit" kibbutz as part of the Battle of #Al-Aqsa_Flood." At 07:34 AM, the Al-Quds Brigades posted a video on Telegram captioned "Al-Quds Brigades Target a Zionist Vehicle at the Nahal Oz Site."

97. On October 11, 2023, the PIJ boasted on its Telegram channel that its "[e]lite companies continue clashing with enemy forces in Zikim."

98. The October 7 Terrorist Attacks amounted to the largest massacre of Jews since the Holocaust and one of the worst terrorist attacks in world history in terms of fatalities. The barbarism and cruelty of the October 7 Terrorist Attacks repulsed the civilized world. As President Biden stated in a speech on the afternoon of that day:

> Hundreds — hundreds of young people at a music festival of — the festival was for peace — for peace — gunned down as they ran for their lives. Scores of innocents — from infants to elderly grandparents, Israelis and Americans — taken hostage. Children slaughtered. Babies slaughtered. Entire families massacred. Rape, beheadings, bodies burned alive. Hamas committed atrocities that recall the worst ravages of ISIS, unleashing pure unadulterated evil upon the world.

99. Reportedly, the Hamas terrorists carried with them detailed maps of Israeli kibbutzim as well as an Israeli military base, which could only have been compiled with "inside knowledge" – almost certainly from Hamas spies. The extraordinary detail and sheer scale of the preparation for the attacks have reportedly led Israeli military officials to conclude that Hamas engaged in many years of planning for the October 7 Terrorist Attacks. Indeed, Israeli officials obtained a detailed copy of Hamas' battle plan for October 7 more than a year before it happened.

100. PIJ was significantly involved in the October 7 Terrorist Attacks. Since 1984, PIJ has been carrying out armed attacks against Israel through its Al Quds Brigade, PIJ's "elite" terrorist division. It is an armed resistance movement that eschews any political compromise in favor of terrorist attacks to bring about the destruction of Israel.

101. Starting in 2020 and continuing through September 2023, both Hamas and PIJ participated in large joint training exercises code-named the "Strong Pillar" drills, which trained the groups to coordinate in attacks against Israeli targets.

102. PIJ and Hamas are united in the war against Israel and have formally coordinated military training. This includes with respect to the October 7 Attacks, a joint effort whose overall success was achieved by Hamas and PIJ cooperation.

103. In September 2023, Hamas and PIJ started a joint operations room in Beirut, Lebanon to organize the October 7 Attacks. PIJ and Hamas cooperated in the massive first assault wave which included the attacks at Kibbutz at Nahal Oz, from where Plaintiff Judith Raanan was taken, the Israeli military base at Zikim and the Kibbutz at Sufa, Israel, and other attacks described earlier in this Complaint, among many other locations in Israel. A PIJ terrorist captured in Gaza admitted that his squadron raped and murdered victims in the October 7 Attacks.

104. PIJ has released at least four statements about its involvement and cooperation with Hamas's Al-Qassam Brigades attacks on October 7. For example, on October 7, 2023, the Telegram channel of the PIJ's Al-Quds Brigades published a statement from its spokesman Abu Hamza, stating: "We are part of this battle and our fighters are shoulder to shoulder alongside their brothers in the Qassam Brigades. Al-Qassam until victory, god willing."

Iran's Multi-Decade Sponsorship of Terrorism

105. Iran has been sponsoring terrorism against the United States and Israel for over three decades, often through proxies such as Hamas and PIJ. Iran has repeatedly been found liable in U.S. courts for deaths and injuries of U.S. citizens caused by its activities as a state sponsor of international terrorism.

106. Over the past few decades, Iran has emerged as the principal backer of Hamas and PIJ terrorism. After Hamas's violent takeover of Gaza in 2007, Iran's support for Hamas terrorism escalated. According to a 2010 U.S. Department of Defense report, Iran provided Hezbollah and several Palestinian terrorist groups—including Hamas—with funding, weapons, and training to attack Israel and disrupt the Middle East peace process.

107. After the conflict between Hamas and Israel in 2014, Iran again increased its funding to Hamas and also began providing Hamas with missile technology as well as materials to construct and rebuild tunnels used for smuggling and terrorist attacks. This included frequent and routine transfers of tens of millions of dollars from Iran to Saudi Arabia and then to Hamas, or transfers from Iran to Hezbollah in nearby Lebanon and then to Hamas.

108. In recent years, Iran, Hamas, and PIJ have adopted cryptocurrencies as a clandestine terrorism funding mechanism. According to a November 12, 2023 expose in *The Wall Street Journal* (entitled *Hamas Needed a New Way to Get Money From Iran. It Turned to Crypto*):

> Initially, Hamas used crypto only to receive small-scale donations from supporters as part of a broader crowdfunding effort, which Israeli officials said has likely raised several million dollars. Around 2020, crypto became a method of large-scale transfers between Iran and the group within the hawala networks. . . .

109. In 2021, Israeli military intelligence reportedly traced tens of millions of dollars in cryptocurrency transfers from Iran to Hamas to buy weapons and pay fighters.

110. According to Reuters, Iran has utilized the cryptocurrency Tron to evade sanctions implemented by the United States. Specifically, between 2018 and 2022, Iranian firms used Tron to conduct $8 billion in transactions, which led Israel's NBCTF to seize 56 Tron "wallets" that it determined were linked to Hamas. Of the 56 Tron wallets, 46 were connected to a single Gaza-based money exchange company called Dubai Co. for Exchange, which Israel considers a terrorist organization because it sends tens of millions of dollars to the military arm of Hamas annually.

111. On January 22, 2024, the U.S Treasury Department further exposed the close financial ties between Iran and Hamas's terrorist activities when it sanctioned, among others, "Gaza-based moneychanger Zuhair Shamlakh" for, among other things, facilitating the transfer of tens of millions of dollars between Iran, Hamas, and other terrorist organizations.

112. According to the 2022 U.S. State Department's Country Report on Terrorism, "[i]n 2022, Iran continued providing weapons systems and other support to Hamas and other U.S.-designated Palestinian terrorist groups, including PIJ . . . These groups were behind numerous deadly attacks originating in Gaza and the West Bank."

113. As has been extensively reported, Iran in recent years has helped Hamas and PIJ develop more advanced rockets to strike Israel as well as assisting with the building of rocket-production facilities in the Gaza Strip. Hamas commanders routinely traveled to Iran to receive training in the production and operation of weapons and to tour the Islamic Revolutionary Guard

Corps's ("IRGC") own rocket-production facilities. Reportedly, the close collaboration between Iran and Hamas has resulted in significant improvements in terms of range, precision, lethality, and the extent of destruction that Hamas's weapons can cause.

Iran's Material Support For Hamas and PIJ In the October 7 Terrorist Attacks

114. As reported by *The Wall Street Journal*, since August 2023, the IRGC worked with Hamas to plan the October 7 Terrorist Attacks at a series of meetings held in Beirut, Lebanon.

115. As many experts have indicated, Hamas cannot and does not launch terrorist attacks without prior explicit agreement from Iran. Indeed, some experts (such as former National Security Adviser John Bolton) have stated that the October 7 Terrorist Attacks marked the beginning of an Iranian strike against Israel, carried out by Tehran's terrorist proxies including Hamas.

116. As *The Wall Street Journal* reported on October 25, 2023, "[i]n the weeks leading up to Hamas's [October 7] attacks on Israel, hundreds of the Palestinian Islamist militant group's fighters received specialized combat training in Iran." The *Journal* further reported that approximately 500 Hamas militants reportedly attended advanced exercises and trainings in Iran in September 2023 led by the IRGC, which may have supported Hamas's use of drones, paragliders, and motorcycles during the October 7 Terrorist Attacks.

117. Similarly, a group of Hamas fighters were reportedly sent to Iran to complete a training with the "Godfather" of Iranian ballistic missile program, Commander Hassan Tehrani-Moghaddam. Captured Hamas terrorists reportedly revealed to Israeli forces that they had been training for the October 7 Terrorist Attacks for a year and were instructed by Iran's IRGC and Hezbollah. The training reportedly included instruction on paragliding and hostage taking.

118. Likewise, Iran reportedly helped plan the attack, select the timing of it, trained militants, and had at least one year's advanced knowledge of it.

119. Likewise, PIJ received direct training from Iran to increase the lethality of its terrorist attacks. In January 2024, a PIJ commander admitted to Israeli intelligence that he and other PIJ terrorists were sent to a 15-day sniper training course at an Iranian-controlled military base in Iran. The commander also admitted that he and other PIJ fighters received artillery and officer command training in Iran.

120. As of December 2023, the IRGC claimed ownership of the October 7 Terrorist Attacks.

121. As many experts had previously reported, Hamas's more sophisticated military capabilities, including its use of drones, paragliders, and hostage taking tactics, are hallmarks of Iran's involvement.

122. As *The Washington Post* reported, more than a dozen intelligence analysts and military experts expressed astonishment at the stealth and sophistication of the Hamas assault, which involved coordinated raids across the Israeli border by hundreds of gunmen traveling by land, sea, and air — including motorized paragliders. The ground offensive was accompanied by swarms of rockets and drones that began streaking across the border early Saturday, hitting targets with a degree of precision not seen in previous Hamas attacks. The intelligence analysts and military experts noted that while Hamas has a capable militia and indigenous assembly lines for rockets and drones as a result of the decades of state sponsorship, the October 7 Terrorist Attacks would have been extremely challenging without considerable outside help.

123. Further underscoring the depth of Iran's involvement, on November 14, 2023, in the third round of sanctions since the October 7 Terrorist Attacks, the U.S. Treasury Department

determined that Iran transferred "tens of millions of dollars" to Hamas by utilizing "the Lebanon-based money exchange company Nabil Chouman & Co ("Chouman") to transfer money from Iran to Gaza."

124. The U.S. Treasury Department also determined in its November 14, 2023 sanctions that Iran "trained Palestinian Islamic Jihad fighters to build and develop missiles in Gaza" in connection with the October 7 Terrorist Attacks and that Iran transferred hundreds of millions of dollars in financial assistance to PIJ for both weapons and operational training.

Syria's Material Support for Hamas and the October 7 Attacks

125. Syria is one of the cradles of Hamas terrorism. Prior to its violent takeover of the Gaza Strip in 2007, Hamas relied heavily on financial support from Syria as well as Iran. Syria has also provided support to the PIJ.

126. Between 2001 and 2012, Syria openly hosted Hamas and PIJ terrorists and provided them with a base of operations in Damascus.

127. In October 2022, Syria hosted a Hamas delegation in Syria and publicly reaffirmed its support for Hamas. Syrian President Bashar al-Assad ("Assad") told the Hamas delegation that: "despite the war that Syria is being subjected to, it did not change its stance of backing resistance by all forms." Assad announced that as "everyone knew before and after the war," Syria "will not change and will continue as a supporter of resistance."

128. Syria materially contributed to Hamas's massive military buildup that preceded the October 7 Attacks. As reported by *Al Jazeerah* in December 2023, Hamas leader Ismail Haniyeh told Al Jazeera that part of Hamas's long-range rocket arsenal comes from Syria.

129. On October 7, 2023, the Assad regime issued a statement immediately praising "Operation Al-Aqsa Flood," the name that Hamas gave to its terror attack of that day. The

statement indicated that: "Syria raises its head high in honor of the martyrs of the Palestinian revolution and the heroes who planned and achieved the Al-Aqsa Flood operation."

130. Syria also abetted the October 7 Terrorist Attacks by supplying Hamas with Captagon, a synthetic amphetamine-type drug.

131. Syria permits the PIJ to locate its headquarters in Damascus.

Hamas And Other Terrorist Groups' Use of Cryptocurrency

132. According to the Financial Crimes Enforcement Network ("FinCEN"), a bureau of the U.S. Department of the Treasury, Hamas raises funds to support its operations and members in a variety of ways, including through: (i) support from Iran; (ii) private donations; (iii) a global portfolio of investments; (iv) diverting aid and support from legitimate charities; (v) the control of border crossings and avenues of commerce; (vi) racketeering business frameworks; (vi) extortionary practices around local populations; and (viii) fundraising campaigns involving crypto currency and fictitious charities raising crypto currency.

133. A significant source of funding for Hamas concerns this last category – cryptocurrency. In addition to facilitating large-scale transfers of funding from Iran, crypto is used by Hamas and PIJ for direct funding. Matthew Price, a former Internal Revenue Service investigator and strategic enforcement lead with crypto analysis firm Elliptic told *The Wall Street Journal* in October 2023 that Hamas has been increasingly using cryptocurrencies to supplement Iran funding because it is "much easier than smuggling cash over Egypt's border."

134. Since at least early 2019, Hamas's al-Qassam Brigades have used cryptocurrency as a fundraising method to support their military operations. In January 2019, a spokesman for the al-Qassam Brigades announced on the group's official Telegram channel that its supporters should use Bitcoin to finance "the resistance," stating the following:

> The Zionist enemy combats the resistance [i.e., Hamas] by attempting to stop the support [it receives] by any means, but the supporters of the resistance in the entire world are fighting these Zionist's attempts and are seeking to find all possible means to support it... We call upon all supporters of the resistance and aides of our just cause to support the resistance financially through Bitcoin using mechanisms that we will soon publish.

135. Hamas and other terrorist groups have used cryptocurrency to support their terrorist activities since 2019 and up to the October 7 Terrorist Attacks. As reported by *The Wall Street Journal* in March 2024, United States Deputy Secretary of the Treasury Wally Adeyemo, sent a letter to Congress indicating that the U.S. Treasury Department is investigating $165 million in reported cryptocurrency transactions that may have helped finance the October 7 Terrorist Attacks.

136. After the October 7 Terrorist Attacks, terrorist organizations, including Hamas and PIJ, continued to use and solicit cryptocurrency to fund their operations. Their use of cryptocurrency and their reliance on the financial exchanges that transact these currencies, such as Binance, continues to this day.

137. Terrorist organizations such as Hamas and PIJ use crypto in other ways as well. Crypto analytics firm Elliptic stated in August 2023 that it found that major terrorist groups including Hamas's al-Qassam Brigades have been using crypto assets for "an ever-growing range of objectives" beyond public fundraising, including sanctions evasion, cybercrime, extortion, investment trading and internal value transfers. Elliptic identified wallets, including Hamas-affiliated wallets, receiving proceeds from sources including stolen credit card vendors, dark web markets, Ponzi schemes and crypto investment scams.

138. Crypto may be used like any other currency to facilitate purchases. It can also be converted into traditional currencies for purchases. In October 2023, Deputy Treasury Secretary Adeyamo stated that identifying these points of exchange into traditional currencies is a big part of the agency's work.

Binance's Business Model

139. Binance is a cryptocurrency platform and exchange. It holds itself out as the world's "largest crypto exchange by trade volume" and was reported to have amassed over half of the global market share for digital asset exchange activity as of the end of 2022. Binance generates revenue by charging users fees in connection with transactions processed on its exchange. In 2021 and 2022, Binance reported approximately $20 billion and $12 billion in revenue, respectively.

140. Binance's primary online virtual currency exchange is operated on the Binance.com platform. On this platform, users may trade fiat (government-issued and backed currency) or virtual currency through a variety of arrangements, including spot, futures, derivatives, and margin trading. To use Binance, a user must open a Binance account and fund the account by depositing assets, either through a virtual currency or fiat currency deposit. Upon onboarding, Binance users can transact in hundreds of virtual currencies and financial products using the funds in their Binance-hosted "wallets." User funds are held in omnibus digital wallets that are visible on public blockchains. Binance acts as the custodian of the user funds and therefore once funds are pooled in those wallets, information about whose money is being moved out of those wallets, as well as any internal transactions between wallets, is not visible to the public. That information is instead recorded on a non-public internal Binance ledger. As the *Global Investigations Review Anti-Money Laundering Guide* notes, "Although many cryptocurrency transactions are indeed recorded on public blockchains, many are not, especially those that take place on centralised exchanges."

141. Binance customers may place orders on www.binance.com, through a Binance mobile application and by direct connection to Binance's matching engines via the Binance application programming interface ("API"). API connections are generally used by more

technologically-sophisticated customers, such as proprietary trading firms or other institutional market participants.

142. Binance operates through a number of subordinate or affiliated entities, in multiple jurisdictions, all tied to Zhao as the beneficial owner. According to the SEC's June 2023 complaint against Binance and Zhao in the District of Columbia, Zhao has publicly dismissed "traditional mentalities" about corporate formalities and has refused to identify the headquarters of Binance, claiming, "Wherever I sit is the Binance office. Wherever I meet somebody is going to be the Binance office." As the SEC set forth in its complaint, according to Zhao, a formal corporate entity with a headquarters and its own bank account is unnecessary: "All of those things [don't] have to exist for blockchain companies."

Identifying Transactions Between Terrorist Organizations and Binance

143. Users may transfer cryptocurrency from their wallets to Binance's omnibus wallets. These transfers are recorded and publicly visible on various cryptocurrencies' blockchain ledgers. Using the Binance exchange interface, users may then use the balance of their Binance accounts for various transactions such as the purchase of fiat currencies (such as dollars) and cryptocurrencies, as well as the purchase of goods and services. These transactions are recorded on internal Binance ledgers and are therefore not visible to the general public. Users may also withdraw the contents of their accounts. If that withdrawal takes the form of cryptocurrency, its transfer from one of Binance's omnibus wallets to the user's private wallet is also recorded on the public blockchain ledger.

144. Cryptocurrency transactions are pseudonymous, not anonymous. A wallet may be identified on the blockchain ledger by only its alphanumeric code. However, because of the nature of cryptocurrency transactions, that wallet's transactions with other pseudonymous wallets are

recorded publicly. Once a pseudonymous wallet code is associated with a real-world entity or person, such as Binance or Hamas, the wallet's interactions are no longer secret.

145. To that effect, government regulators and individuals such as Plaintiffs have learned a significant amount about Binance's interactions with specific third parties, such as terrorist organizations, by reviewing public blockchain information. Because Binance's omnibus wallets have been identified (de-pseudonymized), and many Hamas and PIJ wallets have been de-pseudonymized, it is possible to—as Plaintiffs have done here—identify at least some of the transactions between Binance and terrorist organizations, including Hamas and PIJ.

146. As noted by the *Global Investigations Review Guide to Anti-Money Laundering*, "[a] critical component of [customer] onboarding and KYC is wallet screening" which is facilitated in part by using public blockchain information to "pinpoint[] a wallet's source and destination of funds" as well as "making links with other crypto wallets on the network" in order "to detect if a specific crypto exchange, sanctioned entity or darknet market is in control of a wallet." The *Guide* also identifies transaction monitoring as a key component of an effective anti-money laundering program.

147. Numerous companies have offered blockchain transaction monitoring services expressly for AML compliance to businesses that deal in crypto for years. For example, in November 2019 one such company, Elliptic, told crypto publication CoinDesk that it would be providing such services to the Zilliqa blockchain, noting that "[o]ur tools enable these services to identify whether funds are being laundered through their businesses, by tracing each crypto-asset transaction all the way through the blockchain, to its source . . . . If this source is one of the illicit wallets we have previously identified, the business is alerted and can take steps to prevent the money laundering from taking place."

148. Binance announced that at least one of its entities was using the services of another such company, TRM Labs, in December 2021, "to screen for high-risk wallets, and monitor and investigate suspicious transactions." Binance touted TRM's "best-in-class" "risk assessment, and forensics technology" as a mechanism to "manage regulatory and reputational risk related to digital assets."

149. U.S. regulators have themselves issued guidance recommending the use of such third-party services in order to effectively comply with U.S. law. For example, in October 2021 OFAC issued a sanctions compliance guidance publication for the virtual currency industry. OFAC therein noted that "[a]n effective sanctions compliance program will include . . . controls to identify, interdict, escalate, report (as appropriate), and maintain records for transactions or activities prohibited by OFAC-administered sanctions" and "will enable a company to conduct sufficient due diligence on customers, business partners, and transactions and identify 'red flags.'" The sophisticated data-aggregating and analysis capabilities of third-party providers often enable them to identify particular crypto wallets as risky or even terrorist-related long before the U.S. or other government identifies a wallet as belonging to a terrorist group or other sanctioned entity. For example, if a new or unknown wallet is identified by the third-party provider as having engaged with many prior transactions with known Hamas wallets, the third-party provider may flag the new wallet as very high risk or potentially Hamas-related, warranting further review. This information is made available to customers of third-party service providers, such as Binance, in order for them to conduct required risk assessments of potential customers and transactions and to facilitate mandated reporting to U.S. authorities.

150. OFAC further noted in its guidance that "internal controls often involve the use of industry-specific tools, such as screening, investigation, and transaction monitoring," and that

third-party service providers such as Elliptic and TRM "can be helpful tools for an effective sanctions compliance program."

151. According to Binance's settlement with FinCEN, Binance employed the services of one such third-party provider (potentially TRM) and that provider did alert Binance to transactions involving Hamas occurring on the Binance exchange. It is unknown whether the third-party provider played any role in any customer identification program given that Binance eschewed such requirements of U.S. law. Binance however did have access to both publicly available blockchain information and to sophisticated third-party service providers who could have also identified the transactions identified by Plaintiffs as well as transactions done by any customer of Binance including the other terrorist entities at issue in this matter, and, given the sophisticated data-gathering and analysis capabilities described above, may have and likely did alert Binance that transactions or wallets were connected to Hamas or PIJ long before the U.S. and Israeli government identified, seized and sanctioned specific wallets. Discovery into Binance's use of third-party transaction monitoring services will provide further information on when Binance was aware that particular wallets were or likely were being used to facilitate Hamas' and PIJ's terrorist objectives.

152. Setting aside what Binance knew from third-party monitoring services, Binance processed transactions involving PIJ wallets that had been affirmatively identified by *government sources*. For example, on November 22, 2022, wallet TXBMWt3T4WhFkcPnob1567cGDM3ou27GWE, a PIJ-owned wallet identified by the Israeli National Bureau for Counter Terror Financing ("NBCTF")[1] transferred 201,809 Tether Tokens—approximately $ 201,809 USD—to wallet TTTSEpcsZgqjgqVpwaLp2PZy41TGC1puCG, upon

[1] "Administrative Seizure Order (ASO – 34/23) Anti-Terrorism Law 5776-2016," Israeli Ministry of Defense, July 4, 2023, p. 2, https://nbctf.mod.gov.il/he/Announcements/Documents/%d7%a6%d7%aa%2034-23.pdf.

information and belief a Binance wallet, in a transaction identified on the ledger as c477f66cbf820603c0a787ed90a9a419b9a79d4321c439f17561ca218e6c78f8. [2] Other similar examples exist.

153. Notably, these transactions are likely just the tip of the iceberg as to terrorist organizations' transacting on Binance before the October 7 Terrorist Attacks, as set forth more fully below. Indeed, Binance's internal ledgers are a "black box" that may contain many more transactions that are not recorded on the public ledgers of cryptocurrencies. For example, if Hamas were to purchase dollars on the Binance exchange and then transfer those funds to a conventional bank, it would not be recorded publicly. Additionally, if Hamas were to make a payment to an arms dealer through Binance's exchange, the ledger would record the outgoing flow of cryptocurrency from a Binance omnibus wallet. However, one without access to Binance's ledger would have difficulty discerning, even if the arm's dealers' private wallet were de-pseudonymized, which of Binance customer's funds were used to purchase arms. Finally, if, by using the Binance exchange, other Binance customers made donations to Hamas' fundraising entities that were also customers of Binance, those donations would only appear on Binance's black box internal ledger.

Binance's U.S. Customers

154. Since its inception, Binance has been doing business in the United States. Between 2017 and 2022, Binance has solicited and served millions of U.S. customers. As set forth in the CFTC's December 2023 consent order against Binance, as of January 2020 approximately 20 percent of Binance's customers were located in the United States.

[2] "Transaction Details - c477f66cbf820603c0a787ed90a9a419b9a79d4321c439f17561ca218e6c78f8," *OKlink*, accessed May 13, 2024, https://www.oklink.com/trx/tx/c477f66cbf820603c0a787ed90a9a419b9a79d4321c439f17561ca218e6c78f8.

155. Binance's U.S. customers were critical to its operations and financial bottom line. As a result and as determined by the SEC, the DOJ, and the CFTC, Binance considered many of these U.S. customers to be its high-volume "VIPs." Binance gave these users this moniker because these U.S.-based users were critical for Binance's ongoing operations in that they provided Binance with the critical liquidity it needed to efficiently, cost-effectively, and profitably process trades.

156. By way of background, liquidity is a crucial aspect of financial markets, including the cryptocurrency market. Liquidity refers to the ease with which an asset can be bought or sold without significantly affecting its price. The liquidity of a market impacts trading efficacy and market stability. High liquidity leads to smoother transactions and less price volatility. Low liquidity can result in trading challenges and higher price volatility.

157. High-volume U.S. customers were critical to Binance's ongoing operations, and it broke its own rules to attract and keep them on the exchange. These users functioned as necessary market makers for Binance in that they provided critical liquidity, allowing Binance to effectively function as an exchange. Moreover, these users' high-volume trading generated massive fees and profits for Binance. For example, between 2017 and 2023, Binance maintained over one million U.S. users, who accounted for 15 to 20 percent of Binance's transaction fees, generating billions of dollars in revenue. Indeed, Binance's U.S. users brought massive gains for the company. As FinCEN noted in its November 2023 settlement agreement (described further below), "Binance [] prioritized attracting and maintaining relationships with large U.S. market makers to drive activity on the platform and increase profits" and that "[a]s a result of these actions, Binance now conducts roughly five times the daily trading volume of its next largest competitor" and has "an unfair

competitive advantage in the marketplace as compared to other companies offering similar products and services."

Binance Was Required to Comply with U.S. Laws and Regulations Related to Preventing Funding of Terrorist Groups Such as Hamas and PIJ

158. Given that Binance was conducting substantial business with U.S. users, Binance was at all relevant times required to comply with a wide range of U.S. regulatory requirements and disclosure mandates. Indeed, Binance's long-standing, substantial operations and business with U.S.-based customers subjected it to the jurisdiction of U.S. financial regulators, including the SEC, CFTC and FinCEN and required to comply with U.S. laws and regulations designed to prevent the use of the U.S. financial system to fund terrorist activities.

159. Indeed, since 2011, FinCEN has issued guidance and repeated its position that crypto exchanges such as Binance operating in the United States are money transmission services within the meaning of the Bank Secrecy Act (discussed below) and must therefore register with U.S. regulators and comply with the Act and associated regulations.

160. Pursuant to these laws, Binance was required to put in place necessary internal controls and disclosure requirements. For example, U.S. law required Binance to establish robust anti-money laundering programs, perform due diligence on its customers, file reports of suspicious activity on its platform, and prevent access to the U.S. financial system by sanctioned countries and entities, including terrorists and state sponsors of terrorism.

161. As set forth further below, many of these statutes requiring Binance's compliance with disclosure requirements and internal controls also provide for criminal penalties enforced by the DOJ that could be levied on Binance. The statutes also authorize financial regulators such as FinCEN, the U.S. Department of Treasury, OFAC, the SEC, and the CFTC to promulgate

regulations that aid in civil enforcement, including licensing, reporting, and monitoring requirements on Binance.

International Emergency Economic Powers Act

162. The International Emergency Economic Powers Act ("IEEPA," 50 U.S.C. §§ 1701–05) authorizes the President to declare the existence of an unusual and extraordinary threat to the national security, foreign policy, or economy of the United States. It further authorizes the President to preclude transactions and block the transfer of property to address the threat.

163. U.S. presidents have subsequently issued several executive orders pursuant to this authority to address the threat of terrorism.

164. Between 1995 and 1997, President Clinton relied on IEEPA in issuing Executive Orders 12957, 12959 and 13059 prohibiting virtually all trade and investment activities with Iran because of Iranian support of international terrorism.

165. On September 23, 2001, President George W. Bush issued Executive Order 13224 pursuant to IEEPA declaring a national state of emergency with respect to global terrorism. The order designated a list of individuals and organizations as Specially Designated Global Terrorists ("SDGTs") and authorized the Secretary of the Treasury to further designate other individuals and entities that U.S. intelligence indicated were involved in terrorism.

166. All American persons are barred from having any financial relationship with an SDGT and all SDGTs' U.S.-based assets are frozen. U.S. persons may not engage in financial transactions with an SDGT unless they have obtained a license from OFAC. They also may not engage in any transaction to circumvent this restriction.

167. Violations of an executive order or implementing regulation of IEEPA carry civil penalties. Willful violation is a criminal offense.

The Bank Secrecy Act

168. The Bank Secrecy Act ("BSA") was established in 1970 to combat money laundering, including the financing of terrorist activities. Its provisions are designed to help identify the source, volume and movement of currency transmitted into or out of the U.S. or deposited at financial institutions.

169. The BSA established requirements for recordkeeping and reporting of financial transactions by banks and other financial institutions, including "money services businesses" ("MSB"). The term "money services business" is defined in 31 C.F.R. § 1010.100(ff) to include "money transmitters," which are further defined in 31 C.F.R. § 1010.100(ff)(5) as a person who either "provides money transmission services" or who is otherwise "engaged in the transfer of funds." FinCEN regulations define "money transmission services" as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." Foreign-located businesses are considered MSBs if they do business "wholly or in substantial part within the United States."

170. Under the BSA, MSBs are required to register with FinCEN within 180 days of beginning operations and to renew that registration every two years.

171. Under the BSA and its implementing regulations, MSBs are required to develop, implement, and maintain an effective AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities and to maintain an effective, written AML program that (1) incorporates policies, procedures and internal controls reasonably designed to assure ongoing compliance with the BSA and its implementing regulations; (2) designates an individual responsible to assure day-to-day

compliance with the program, the BSA and BSA regulations; (3) provides education and/or training for appropriate personnel, including training in detection of suspicious transactions; and (4) provides for independent review to monitor and maintain an adequate program.

Suspicious Activity Reporting

172. The BSA and its implementing regulations require an MSB to identify and report suspicious transactions relevant to a possible violation of law or regulation in Suspicious Activity Reports ("SARs") filed with FinCEN. Specifically, the BSA and its implementing regulations require MSBs to report transactions that involve or aggregate to at least $2,000, are conducted by, at, or through the MSB, and that the MSB "knows, suspects, or has reason to suspect" are suspicious. A transaction is "suspicious" if an MSB "knows, suspects or has reason to suspect" the transaction: (a) involves funds derived from illegal activities, or is conducted to disguise funds derived from illegal activities; (b) is designed to evade the reporting or recordkeeping requirements of the BSA or regulations implementing it; or (c) has no business or apparent lawful purpose or is not the sort in which the customer normally would be expected to engage, and the MSB knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction. An MSB is generally required to file a SAR no later than 30 calendar days after the initial detection by the MSB of the facts that form the basis for filing a SAR.

173. Laws and regulations pertaining to other types of financial market participants include provisions bringing them within the scope of the BSA. For example, Regulation 42.2 of 17 C.F.R. § 42.2 requires commodities exchanges to comply with the BSA. Rule 17a-8 of the Securities Exchange Act of 1934 requires broker-dealers to comply with the reporting, recordkeeping, and record retention rules of the BSA.

Binance's Scheme To Avoid U.S. Regulations And Supervision

174. Binance sought to secretly do business with United States customers while ignoring U.S laws and thereby avoid the scrutiny that accompanies U.S. banking, financial, and anti-terrorism regulations. As a result and beginning years ago, Binance engaged in a scheme to retain its U.S. users while concealing that these users had access to Binance.com, creating a culture at Binance of contempt and mockery for U.S. regulatory supervision, with Binance engaging in widespread violations of U.S. law.

175. Binance sought to evade U.S. regulatory oversight through an elaborate scheme by which Binance created U.S. entities and a separate platform, Binance.US (available at www.binance.US), which Binance held out as its official U.S. crypto exchange. Binance misrepresented to the public, U.S. authorities, and U.S. courts that Binance.US was the exclusive platform on which U.S. persons could trade on Binance.

176. But this was a lie. Behind the scenes and as referenced above, Binance engaged in a scheme to retain its most valuable U.S. customers on the Binance.com platform without disclosing these customers' U.S. locations. When the Binance.US platform launched in 2019, Binance announced that it was implementing controls to block U.S. customers from the Binance.com platform. In reality, Binance did the opposite. As both the CFTC and the SEC concluded in their respective complaints against Binance a Zhao, in March and June 2023, respectively, Zhao directed a scheme by which Binance would assist high-value U.S. customers in circumventing those controls and to do so surreptitiously because—as Zhao himself acknowledged—***Binance did not want to "be held accountable"*** for these actions. (Emphasis added).

177. As the SEC set forth in its June 2023 complaint, Binance's CCO explained, ***"[o]n the surface we cannot be seen to have US users[,] but in reality, we should get them through other creative means***." (Emphasis added). Indeed, and as admitted by Binance's Chief Compliance Officer ("CCO"), per Zhao, Binance would engage in "***the international circumvention of KYC***," so that Binance could "***reduce the losses to ourselves, and at the same time to make the U.S. regulatory authorities not trouble us***." (Emphasis added).

178. On a June 2019 Binance conference call, Binance employees and executives confirmed to Zhao that they were implementing his scheme. As concluded by the U.S. Attorneys' Office for the Western District of Washington in its criminal information against Binance, these employees told Zhao that they had been contacting U.S. VIP users "offline," through direct phone calls, "***leav[ing] no trace***." (Emphasis added). If a U.S. VIP user owned or controlled an offshore entity, i.e., located outside of the United States, Binance's VIP team would help the VIP user register a new, separate account for the offshore entity and transfer the user's VIP benefits to that account, while the user transferred its holdings to the new account. On the same call, an employee described a script that Binance employees could use in communications with U.S. VIPs to encourage them to provide non-U.S. KYC information to Binance by falsely suggesting that the user was purportedly "misidentified" in Binance's records as a U.S. customer.

179. Also during this June 2019 conference call, a senior employee provided guidance on what Binance should not do. As set forth by the U.S. Attorneys' Office for the Western District of Washington in its criminal information against Binance, the employee stated that: "We cannot advise our users to change their KYC. That's, that's of course against the law." The senior employee provided an alternative route to the same end: "But what we can tell them is through our internal monitoring, we realize that your account exhibits qualities which makes us believe it is a

US account ... if you think we made a wrong judgment, please do the following, you know, and we have a dedicated customer service VIP service officer." The senior employee described Binance's plan as "***international circumvention of KYC***." (Emphasis added).

180. As CEO, Defendant Zhao supervised and directed this misconduct. For example and as determined by the U.S. Attorney's Office for the Western District of Washington in its criminal information against Binance, Zhao authorized and directed Binance's strategy of purportedly "mischaracterizing" its users' locations, explaining on a June 2019 call with Binance employees that "[w]e cannot say they are U.S. users and we want to help them. We say we mis-categorized them as U.S. users, but actually they are not." Likewise, Zhao directed Binance to implement a plan to encourage customers to circumvent U.S. IP-blocking controls. Moreover, Zhao directed Binance employees to encourage certain U.S.-based VIP customers, including VIPs located in New York, to circumvent KYC restrictions by submitting updated KYC information that deleted any U.S. nexus. An internal document titled "VIP handling" makes clear that Zhao directed this scheme.

181. Zhao knew that he and Binance were breaking the law. As part of his November 2023 guilty plea with the DOJ, Zhao admitted to willful violations of the Bank Secrecy Act. Zhao admitted he was aware of the presence of significant U.S. business on his trading platform and the concurrent requirements to comply with U.S. laws, including those pertaining to customer due diligence, monitoring and reporting designed to prevent known terrorist organizations from transacting on the Binance platform. Notwithstanding this knowledge and as the U.S. Attorney's Office for the Western District of Washington in its criminal information against Binance set forth, Zhao nevertheless told Binance employees that, when it came to compliance with U.S. law, it was "***better to ask for forgiveness than permission***." (Emphasis added). Zhao later acknowledged the

seriousness of his crimes, in allowing among other things terrorist groups like Hamas to operate freely on Binance, and apologized for his crimes at his sentencing hearing on April 30, 2024.

Binance and Zhao Created and Operated a Platform That Enabled Financing and Other Transactions for Terrorist Groups, in Violation of U.S. Anti-Terror Financing Regulations

182. As a result of Binance's scheme, illicit actors including Hamas and PIJ freely transacted on its platform. Binance knew, remained willfully blind, and affirmatively assisted the use of its platform by illicit actors, including terrorists. Indeed, Binance intentionally created a financial ecosystem on which it could provide services to illicit actors so they could freely transact without fear that Binance would otherwise block their transactions or report them to governmental authorities.

183. Binance's creation of a free-for-all financial ecosystem for criminals is reflected by Binance's account levels. As the U.S. Attorney's Office for the Western District of Washington set forth in its criminal information of Binance, prior to August 2021, Binance allowed users to open "Level 1" or "Tier 1" accounts without submitting any KYC information whatsoever. Instead, users could open Level 1 accounts simply by providing an email address and a password. Binance required no other information, including the user's name, citizenship, or location. A Level 1 account holder could deposit virtual currency into its account, and then transact in, an unlimited amount of virtual currency. While Level 1 accounts had certain limitations, including a virtual currency withdrawal limit of up to the-value of two Bitcoins ("BTC") per day, Binance allowed users to open multiple Level 1 accounts by providing a new email address for each account, which effectively circumvented the withdrawal limit. Even if a user adhered to the daily two BTC withdrawal limit on a single account, for most of Binance's existence, the user could still withdraw thousands-and sometimes many tens of thousands-of U.S. dollars due to the rising value of a single Bitcoin, which increased from approximately $3,000 to $63,000 in value between December 2018

and April 2021. Level 1 accounts comprised the vast majority of user accounts on Binance.com. These Level 1 accounts were effectively playgrounds for terrorists and criminals to secretly transfer illicit funds.

184. After August 2021, when Binance first began performing customer due diligence, it built a platform regulatory compliance program that by design still contained massive gaps to allow criminal activity to take place. Notwithstanding that, in August 2021, Binance announced that it would require all new users to submit full KYC information, Binance nevertheless allowed existing users who had not previously submitted KYC information – including all Level 1 accounts (which were the majority of Binance's user accounts) – to trade on the platform without providing full KYC information until May 2022. In other words, the platform was still usable for terrorist entities with existing Level 1 accounts.

185. Binance personnel had actual knowledge that illicit activity was flowing through the platform as the result of these deficient KYC procedures. For example and as detailed by the U.S. Attorney's Office for the Western District of Washington, in a September 2018 chat conversation, a senior Binance employee learned that Binance had "[n]othing ... in place" to review high-volume accounts for suspicious activity. In the same chat, he listed types of transactions that, "in [the] aml world," would be flagged for money laundering risks, while noting that "as of now[,] there is no regulation for .com to play by."

186. Binance purposefully created a platform without legally-required internal controls in place to flag and report illicit transactions in order to attract maximum trading activity and did not alter its practice despite knowledge of subsequent and foreseeable illegal trading activity. For example and as set forth by U.S. Attorney's Office for the Western District of Washington in its criminal information against Binance, in 2018, a Binance senior employee noted: "its [sic]

challenging to use the aml standards to impose on [Binance].com ***especially when Cz [Zhao] doesn't see a need to***." (Emphasis added).

187. Binance's culture of promoting a platform so that it could provide services to terrorists and criminals continued for years. As set forth by the CFTC in its March 2023 complaint against Binance and Zhao, in 2020, Binance's CCO, in response to having been presented with evidence of criminal transactions on its exchange, admitted that bad actors were using Binance, stating "***Like come on. They are here for crime***." Binance's comically-mistitled Money Laundering Reporting Officer agreed, commenting "***we see the bad, but we close 2 eyes***." (Emphasis added).

188. The culture of enticing terrorists and criminals to use their financial and cryptocurrency services was part of Binance's business model. As set forth by the U.S. Attorney for the Western District of Washington in its complaint against Binance, one compliance employee wrote, "we need a banner '***is washing drug money too hard these days - come to binance we got cake for you***.'" (Emphasis added). Indeed, terrorist groups like Hamas and PIJ felt comfortable to launder tens of millions of dollars through Binance.

189. And to that effect, Binance took steps to retain known illicit actors on the platform, particularly if they were VIP users. For example, in July 2020 and as detailed by the U.S. Attorney for the Western District of Washington in its complaint against Binance, Binance's chief financial officer ("CFO") and others discussed a VIP user who was offboarded after being publicly identified as among the "top contributors to illicit activity." The CFO wrote that, as a general matter, Binance's compliance and investigation teams should check a user's VIP level before offboarding them, and then Binance could "give them a new account (if they are important/VIP)" with the instructions "not to go through XXX channel again."

190. Binance's willful failure to implement an effective AML program directly led to criminal activity. As FinCEN concluded in its consent order against Binance, Binance's knowing failure to implement an effective AML program led to the exchange "being used to process transactions related to . . . unregistered convertible virtual currency mixing services used to launder illicit proceeds, high-risk jurisdictions, individuals listed on OFAC's SDN List, ***[and] terrorist financing***." (Emphasis added). FinCEN determined that Binance's willful failure to report hundreds of thousands of suspicious transactions "inhibited law enforcement's ability to disrupt the illicit actors" and that its conduct "extensively harmed FinCEN's mission to safeguard our financial system from illicit use" and "expos[ed] the U.S. financial system to a significant volume of illicit financial activity." Similarly, FinCEN concluded that "Binance senior management misled U.S. authorities," and "***Binance's willful failure to implement an effective [anti-money laundering] program directly led to the platform being used to process transactions related to . . . terrorist financing***," among other illicit activities. (Emphasis added).

191. Reflecting the culture of impunity at Binance and its contempt for U.S. regulators, as noted in OFAC's 2023 settlement with Binance (described further below), Binance's deputy head of compliance acknowledged that "[Zhao] keeps saying that compliance is here to make Binance APPEAR compliant." The very top members of Binance management deliberately created the culture of impunity at Binance and its contempt for U.S. regulators and U.S. law.

192. Binance's contempt for U.S. regulators continues through the October 7 Terrorist Attacks and to this day. As *The Wall Street Journal* reported on May 9, 2024, Binance, in U.S. regulators' crosshairs in 2023, promised "unceasing efforts to deliver a safe and trusted platform." However, when confronted by one of its internal investigations with direct evidence of market manipulation conducted by one of Binance's VIP market-making clients, Binance, in late-2023,

fired its investigator and retained its market-manipulating VIP client so that Binance could continue "generating trading fees from large clients over fixing its practices." There is no reason to believe that Binance has reformed itself or will remediate any of its misconduct. Rather Binance will continue to conduct business as usual: allowing criminal activity on its platform, in utter contempt for U.S. regulators and in continued violation of U.S. law.

Terrorist Groups Transacted Millions of Dollars on Binance Leading Up To October 7

193. Given that criminal actors had flocked to Binance and it had closed its eyes to criminal activity taking place on its platform, it is no surprise that terrorist groups transacted money on its exchange. And these terrorist groups, including Hamas and PIJ, did so in massive amounts and with impunity.

194. Leading up to the October 7 Terrorist Attacks, Hamas and PIJ executed thousands of transactions on Binance, with a total value of at least approximately $60 million. From October 2020 to September 2023, Hamas and PIJ wallets transferred approximately $30 million to Binance wallets. The largest of these transactions (ranging from approximately $150,000 to $200,000) were conducted from March to December 2022, in the months leading up to the October 7 Terrorist Attacks. And from October 2020 to September 2023, Binance wallets transferred approximately $29 million to Hamas and PIJ.

195. Other Gaza-based financial services companies affiliated with Hamas including BuyCash and Dubai Co for Exchange ("Dubai Co."; and collectively with BuyCash, Hamas, and PIJ, "Hamas-Affiliated") also executed millions of dollars' worth of transactions on Binance leading up to the October 7 Terrorist Attacks.

196. As to BuyCash and by way of background, BuyCash holds itself out as a remittance company, currency exchanger, money transfer service and electronic bank. Notably in June 2021,

Israel's NBCTF seized a BuyCash wallet that was used for Hamas fundraising. BuyCash and its owner, Ahmed M.M. Alaqad, who is based in Gaza, were designated as providing material support to Hamas. From January 2019 to October 2023, BuyCash wallets transferred approximately $21 million to Binance. The largest of these transactions, ranging from $150,000 to $230,000, occurred in July to September 2023, the months immediately preceding the October 7 Terrorist Attacks. From January 2019 to October 2023, Binance transferred approximately $4 million to BuyCash wallets, with the largest of these transactions occurring between July and early October 2023 – again, in the time period immediately preceding the October 7 Terrorist Attacks. In other words, BuyCash transacted no less than $25 million on Binance leading up to the October 7 Terrorist Attacks.

197. Dubai Co. also executed millions of dollars' worth of transactions on Binance leading up to the October 7 Terrorist Attacks. Dubai Co. is a Gaza-based business that Israel's NBCTF has for years been monitoring and considers affiliated with Hamas. From May 2020 to October 2023, Dubai Co. transferred approximately $3.5 million on Binance, with the largest of these transactions (in the hundreds of thousands of dollars) occurring from March 2022 to September 2022. Likewise, between August 2020 and August 2023, Binance transferred approximately $12.5 million to Dubai Co., with the largest of these transactions occurring from May 2021 to November 2021. In other words, Dubai Co. transacted no less than $16 million on Binance leading up to the October 7 Terrorist Attacks.

198. Accordingly, leading up to the October 7 Terrorist Attacks, these Hamas-Affiliated wallets transferred a staggering amount of money on Binance – at least approximately $101 million.

199. As set forth above, the extent of Binance's transactions with these sanctioned and Hamas-affiliated entities may be greater than is revealed by the public ledger. Binance's publicly-

inaccessible, internal ledgers may reflect additional transactions in both fiat and cryptocurrencies, demonstrating further material support provided by Binance to terrorist organizations involved in the October 7 Terrorist Attacks, including Hamas and PIJ.

Binance Knew That Hamas and Other Terrorist Groups Transacted on Its Platform

200. Binance built and intentionally maintained woefully inadequate internal controls, and created a platform on which it knew illicit actors transacted and transferred money. Binance also knew that it was providing services to terrorist groups such as Hamas and PIJ that were using Binance. Binance deliberately refused to carry out the minimum and required level of scrutiny of its customers, demonstrating the highest level of willful, reckless disregard.

201. These terrorist groups publicly admitted to using Binance's services. For example, Hamas specifically publicized its use of Binance. A video published on the Al-Qassam Brigades' (a particular armed unit of Hamas) website in 2019, which Hamas used to solicit donations, provided the public with an explanation of what cryptocurrency is and how it could be used for donations, advising its viewers to "create a new account on one of the trading platforms" in order to deposit donations.

202. Notably, one of those platforms was Binance, as set forth in the below screenshot of a donation page on the Al-Qassam Brigades' website, archived on June 6, 2019:

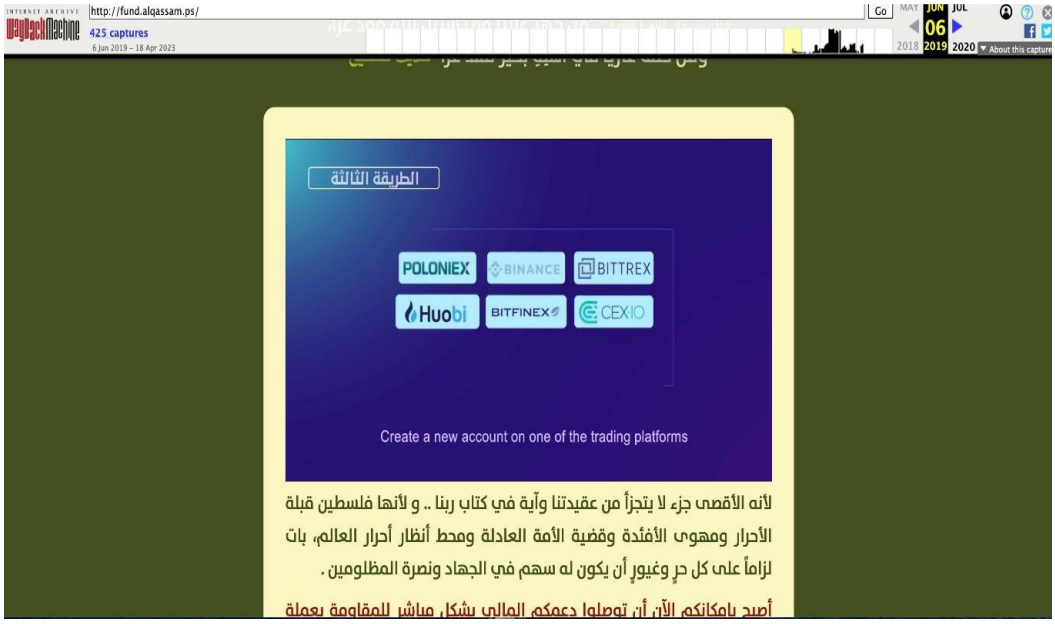

Figure 1: Screenshot of archived video tutorial instructing users to create accounts on one of the trading platforms.

203. Hamas continued to publicly solicit cryptocurrency donations on the Al-Qassam Brigades' social media and website until April 2023. According to MEMRI, "The Al-Qassam Brigades issued a call for Bitcoin donations on April 10, 2023." According to an April 28, 2023 Reuters article, Hamas had issued a statement citing increased interception of funds and concern about the safety of donors and to spare them any harm.

204. After its April 2023 announcement, Hamas increasingly relied on receiving cryptocurrency donations through third-party channels instead of soliciting them through their own social media, increasing Hamas' reliance on cryptocurrency exchanges such as Binance. In discussing recent Hamas crypto-related activity, blockchain analysis specialist Ari Redbord told Public Broadcasting Service (PBS) in November 2023:

> Today, what we're really seeing is since the start of the war. We've seen mostly supporters of Hamas raising funds. And when I say supporters, you know, those celebrating, you know, death to Israeli civilians or promoting different acts of terror or supporting different acts of terror.

205. Similarly, news media publicized terrorist groups' use of Binance. For example, in February 2019, the Israeli online business publication Globes reported that Hamas crypto donations had "received donations from wallets of U.S. trading platforms from Bittrex and Coinbase, ***from Binance […] wallets*** ..." (Emphasis added). That same month, an Israeli blockchain analysis group, Whitestream, flagged that Binance was involved in the chain of Hamas crypto donations on its Twitter account in a post that is dated February 16, 2019, as set forth in the below figure:

Figure 2: Screenshot of Whitestream's February 2019 tweet flagging Hamas' cryptocurrency fundraising campaign on Twitter.

206. By June 2021, flagship financial news media sources publicized an uptick in Hamas' cryptocurrency fundraising, causing Hamas' use of cryptocurrency to become even more well known. According to *The Wall Street Journal* from an article published in June 2021:

> Hamas has seen a surge in cryptocurrency donations since the start of the armed conflict with Israel [in May 2021] … exploiting a trend in online fundraising that has enabled it to circumvent international sanctions to fund its military operations.

207. Additional news media reports from 2021 underscored the increased awareness and scrutiny surrounding Hamas' use of cryptocurrency. For example, on June 4, 2021, the Middle East Media Research Institute's ("MEMRI's") *Jihad and Terrorism Threat Monitor* ("JTTM") published a brief entitled "Jihadis on Using Cryptocurrencies – The Next Threat," which outlined the increasingly common solicitation of cryptocurrency among extremist groups. The article included a summary of Hamas' online fundraising campaign via their website and social media, from which they "regularly shar[e] links on its Telegram channel to a page with new Bitcoin addresses where donations can be sent." Furthermore and following a July 2021 seizure of e-wallets by the Israeli government, the blockchain analysis firm Elliptic published a report outlining the seized wallets, noting that Hamas used a variety of crypto assets including Dogecoin, Ether, and Tether.

208. In September 2021, Coinbase, a cryptocurrency exchange and a business competitor of Binance, published a report noting an escalation in Hamas' cryptocurrency fundraising efforts. Coinbase concluded the report with the pledge to "take three critical steps" to minimize the ability of Hamas and other insurgent groups to use crypto:

> 1. Blocklist [sic.] any crypto addresses associated with these organizations to prevent users from sending funds to them.
>
> 2. Leverage Coinbase Analytics to detect wider terror organization campaign efforts and identify possible participants and accessories.

3. Coordinate with law enforcement and regulatory agencies, such as FinCEN, the FBI, and others.

209. The sheer magnitude of terrorist-associated transactions further confirms Binance's knowledge that terrorists were transacting on its platform. Based on an analysis conducted for Plaintiffs of publicly-available blockchain data from a leading blockchain analysis firm using currently known Hamas and PIJ wallets, Binance processed, at a minimum, thousands of transactions with a total value of at least nearly $60 million involving crypto wallets of Hamas and PIJ between 2019 and September 2023, predominantly in the cryptocurrencies Tether and Tron. That analysis also showed that Binance processed approximately an additional $42.5 million in transactions involving wallets of Gaza-based money-services businesses. One of those services business, BuyCash, has since been designated by OFAC for transmitting money and facilitating donations for Hamas; another services business, Dubai Co. has been identified by Israel as a "terrorist group" "due to the aid that they provide to the Hamas terrorist organization, particularly its military arm, in transferring funds on a scale of tens of millions of dollars a year."

210. Binance also knew terrorists were using its platform as a result of U.S. government investigation and intervention. For example, prior to entering into its settlement with FinCEN in November 2023, ***FinCEN had identified to Binance numerous transactions between Binance users and users with Hamas ties, including the Al-Qassam Brigades and PIJ***. Indeed, senior Binance employees and compliance personnel were aware that entities officially designated as terrorist groups were transacting on the Binance.com platform.

211. Likewise and as concluded by FinCEN in its consent order against Binance, Binance had processed "significant sums" on behalf of Hamas, PIJ and other terror groups:

> ***Binance failed to file SARs with FinCEN on significant sums being transmitted to and from entities officially designated as terrorist organizations by the United States and United Nations***, as well as high-risk exchanges associated with terrorist financing activity. Binance user addresses were found to interact with bitcoin wallets associated with the Islamic State of Iraq and Syria (ISIS), ***Hamas' Al-Qassam Brigades***, Al Qaeda, and the ***Palestine Islamic Jihad (PIJ).***

(Emphasis added).

212. These terrorist-related sums included tens of millions of dollars in transactions with accounts tied to PIJ, with FinCEN concluding in its consent order against Binance that:

> ***FinCEN's investigation identified dozens of former Binance users with tens of millions of dollars in transactions with an identified [Palestinian Islamic Jihad] network***. Binance failed to file a SAR with FinCEN on this activity some of which occurred [between July 14, 2017 to July 30, 2023].

(Emphasis added).

213. As determined by FinCEN and the CFTC in their actions against Binance, Binance was aware that Hamas-affiliated users, including PIJ, were transacting on its platform. Indeed, FinCEN found that ***throughout 2019 and 2020, specifically in April 2019 and July 2020, Binance received reports from its third-party service provider, which identified Hamas-associated transactions***. The third-party service provider is not identified in public documents, but numerous companies hold themselves out as providing robust blockchain analysis features expressly designed to identify illicit activity.

214. In response to these Hamas-associated transactions on its exchange identified by its third-party provider, Binance did not file any SARs as it was required to do so to alert U.S. regulators. Instead and as concluded by FinCEN in its November 2023 consent order, Binance

ignored its regulatory obligations and "***attempted to influence how the service provider reported these transactions***." (Emphasis added). In other words, Binance provided services to Hamas via its exchange and tried to mislead regulators to allow the terrorist activity to continue, and the profits to accumulate.

215. Not only did Binance know that users associated with Hamas were exchanging cryptocurrency on its platform, Binance went out of its way to protect these users and itself from further regulatory scrutiny. Specifically, FinCEN concluded in its November 2023 consent order that:

> [I]n July 2020, after a third-party service provider flagged ***accounts associated with ISIS and Hamas***, [Binance's] former Chief Compliance Officer described it as "[e]xtremely dangerous for our company" and instructed compliance personnel to "[c]heck if he is a VIP account, if yes, to… ***[o]ffboard the user but let him take his funds and leave. Tell him that third party compliance tools flagged him***."

(Emphasis added).

216. The CFTC has also made clear that Binance knew that Hamas had transacted on its exchange. Specifically, the CFTC in its March 2023 complaint against Binance and Zhao set forth that, Binance, in February 2019 received information "***regarding HAMAS transactions***." (Emphasis added). In response to this information, Binance's then-CFO knew so much about terrorists' transacting on cryptocurrency platforms that he explained to a colleague that terrorists usually send "small sums" as "large sums constitute money laundering." A Binance colleague replied that one "can barely buy an AK47 with 600 bucks."

217. Binance also knowingly permitted customers associated with illicit activity to open new accounts and continue trading on its platform. As the CFTC set forth in its complaint against Binance. "***Zhao's business strategy . . . counseled against off-boarding customers even if they***

presented regulatory risk." (Emphasis added). Indeed, Binance's Chief Compliance Officer texted Binance employees: "***Don't need to be so strict***" and "***Offboarding = bad in [Zhao's] eyes***." (Emphasis added).

218. Binance knew of and turned a blind eye to the activities of BuyCash, a Gaza-based money-services entity that raises funds for Hamas and has been designed by OFAC as materally assisting Hamas. Specifically, FinCEN in its consent order found: "Binance also failed to file a SAR with FinCEN on its connections to BuyCash … Prior to OFAC's designation of BuyCash, ***Binance was aware of extensive suspicious activity involving this entity—including connections related to terrorist organizations—but failed to file a SAR with FinCEN***." (Emphasis added).

219. FinCEN concluded that Binance's misconduct as to providing services to terrorists, such as Hamas which transacted on its platform, was knowing and intentional. Specifically, FinCEN concluded, "Binance senior management misled U.S. authorities," and "Binance's willful failure to implement an effective [anti-money laundering] program directly led to the platform being used to process transactions related to . . . terrorist financing," among other illicit activities.

220. Likewise as to Zhao's intentional misconduct, Zhao was personally responsible for causing Binance's misconduct as set forth above, including Binance's facilitation of transactions with Hamas and PIJ.

221. Zhao was well aware of U.S. regulations that were intended to prevent financial intermediaries such as Binance from processing transactions linked to terrorists. As OFAC underscored in its November 2023 settlement with Binance, in June 2019 Zhao told a senior Binance employee that "***the U.S. has this law: you have to prevent Americans and any terrorists from doing any transactions. In order [for America] to accomplish this, if you serve Americans or service American sanctioned countries, you have to give your data to the American***

regulators." (Emphasis added). And notwithstanding of his knowledge of these regulatory requirements, Zhao, through Binance' scheme of avoiding U.S. regulators' oversight, deliberately flouted U.S. law. In his plea agreement with the DOJ, Zhao agreed that "[s]tarting at least as early as August 2017 and continuing to at least October 2022, [he] violated the Bank Secrecy Act . . . ***by willfully causing [Binance] to fail to implement and maintain an effective [anti-money laundering] program***." (Emphasis added).

222. There is far more yet to be unearthed about what Binance and Zhao knew about Hamas's and PIJ's transacting on its exchange before the October 7 Terrorist Attacks. As FinCEN stated in its settlement agreement with Binance, FinCEN had identified "hundreds of thousands of potentially suspicious transactions that went through the Binance platform." These hundreds of thousands of potentially suspicious transactions may give rise to additional facts concerning Binance's scienter and will identify substantial additional transactions that funded Hamas, PIJ and related entities.

223. To that effect, OFAC identified more than $600 million worth of transactions between U.S. persons and crypto wallets located in or otherwise connected with Iran, a significant funding source for Hamas, and tens of millions of dollars of additional transactions between U.S. persons and crypto wallets located in or otherwise connected with Syria, another funding source.

224. Moreover, Binance maintains an internal ledger that is not public and will only be able to be analyzed in discovery that may contain evidence of additional transactions by Hamas, PIJ and associated terrorist groups. Indeed, Binance's CFO was apprised of terror groups transacting on the exchange and had access to the internal ledger.

225. Likewise as to the Israel's investigation and identification of terrorist related wallets on Binance. As the Times of Israel reported, in February 2022, eight months before the October 7

Terrorist Attacks, Israel seized ***12 Binance accounts linked to Al-Mutahadun Exchange, which reportedly "assist[ed] the Hamas terror group, and especially its military wing, by transferring funds***." (Emphasis added).

226. Binance also knew that terrorist groups were using its platform as a result of governments' publications of e-wallets associated with terrorist groups. By way of background, Israel publishes a blacklist of Hamas-affiliated wallets via Israel's NBCTF. The NBCTF website lists all cryptocurrency seized via Administrative Seizure Orders ("ASOs"). Israel justifies these seizures through Israeli Anti-Terrorism Law, in which Israel states that the seized wallets and accounts have been analyzed to be "property of … designated terrorist organizations." To date, this list includes 162 Hamas-affiliated crypto wallets listed from June 2021 to July 2023:

- June 2021: NBCTF listed 84 crypto wallets affiliated with Hamas.
- March 2022: NBCTF listed 47 crypto wallets affiliated with Dubai Co. for Exchange, which Israel alleges transfers funds to Hamas.
- April 2023: NBCTF lists 5 e-wallets associated with Al Mutahadun for Exchange, Dubai Co. for Exchange, and/or Al Wefaq Co. for Exchange. Israel alleges that the three money exchanges transferred funds to Hamas.
- July 2023: NBCTF lists 26 e-wallets associated with PIJ.

Some of these wallets were used to process a portion of the approximately $60 million in Hamas-related transaction on Binance, as alleged above.

227. The United States also tracks and publishes lists of Hamas-affiliated wallets for public information. In the United States, sanctioned wallets are published by the Department of Treasury and the DOJ. Some of these wallets were used to process a portion of the approximately $60 million in Hamas-related transaction on Binance, as alleged above. These lists are compiled

in part by obtaining identifying information regarding the owners of crypto wallets, which are otherwise anonymous.

228. Binance was required by law to obtain such customer-identifying information before allowing customers to transact on its platform, however, for years it deliberately chose not to. Binance and Zhao knew they providing services to and were facilitating transactions for Hamas, PIJ, and other terror groups and that they had the tools to identify and stop the activity. However, they preferred to collect fees and ignore the consequences of their actions. Zhao eventually admitted at his sentencing hearing that he "realized[d]" "the seriousness" of his crimes in allowing, facilitating, and encouraging terror groups and other criminals to freely operate on the Binance platform.

229. The nature of the transactions that FinCEN identified as being associated with Hamas also demonstrates that Binance knew that terrorists were transacting on its exchange. These transactions were either direct transactions between the Binance exchange and the relevant wallets or were part of multi-step transactions that bear indicia of money laundering. As to direct transactions, the tracing of whether the cryptocurrency is flowing from or to a terrorist-associated wallet is a matter of simple and necessary due diligence which any financial institution is required to do. As to the latter category, such indicia include:

- *Graphton*: A graphton is a blockchain analysis term that indicates that funds follow a series of transactions along the blockchain. These transactions share common traits and thus are indicative that the same entity is conducting all transactions.

- *Peeling Chain*: In a peeling chain, an initial sum of cryptocurrency is allocated to a specific address. A fraction of this amount is then siphoned off and transferred to another address, typically destined for deposit at an exchange such as Binance, while the bulk is redirected to a different address linked to the same entity. This sequence recurs until the original cryptocurrency is fragmented into smaller portions. Such a sequence may suggest efforts to obscure the origin and destination of the funds.

230. These transactions bear such indicia of illicit activity and were identified as being associated with terrorist groups using tools available on third-party crypto transaction monitoring platforms. These platforms offer services to financial services firms (including crypto exchanges such as Binance) for the express purpose of identifying suspicious transactions in order to comply with Bank Secrecy Act and other regulatory requirements. FinCEN's settlement agreement with Binance indicates that Binance had access to and did use such a third-party service firm. Indeed, the FinCEN settlement agreement states that the third-party firm alerted Binance to the presence of Hamas transactions on the Binance platform.

231. In addition to wallets listed by governments, third party institutions also publish wallets associated with Hamas on their websites. These reports – which stem from industry reporting, intelligence reports, and traditional news media – extend past sanctioned lists by identifying e-wallets published by Hamas and their affiliates on their social media platforms. Such reporting is exemplified by the following:

- On February 3, 2019, the Meir Amit Intelligence and Terrorism Information Center published a report listing an e-wallet posted on the Twitter account of the Hamas-affiliated Popular Resistance Committees.

- On October 10, 2023, TRM published an article including a number of screenshots of e-wallets posted on Hamas social media.

- On October 23, 2023, the Middle East Media Research Institute published an article detailing Hamas' historical use of cryptocurrency to elicit donations. In the article, MEMRI identifies an Ethereum e-wallet that had posted to Gaza Now's telegram account. Gaza Now allegedly solicited donations to Hamas' military wing, Al-Qassam Brigades, in the aftermath of October 7, 2023.

Binance and Zhao Plead Guilty and Have to Pay a $4.3 billion Penalty for Violating U.S. Law, Including Prohibitions on Transactions for Terrorists and State Sponsors of Terrorism

232. On November 21, 2023 Binance pled guilty to violations of federal law in conducting an unlicensed money transmitting business ("MTB") and failing to maintain an effective anti-money laundering program. Binance entered into concurrent settlements with OFAC, FinCEN, and the CFTC for various willful violations of IEEPA, the Bank Secrecy Act, and related regulations, including for failing to implement a Customer Identification Program, "Know Your Customer" ("KYC") policies and procedures, and AML program, failure to retain required customer information, and failure to implement procedures to determine whether a customer appears on lists of known or suspected terrorist organizations.

233. On November 21, 2023, Binance and Zhao entered into a comprehensive settlement with the DOJ Criminal Division, the U.S. Attorney's Office for the Western District of Washington, FinCEN, OFAC, and the CFTC to resolve years-long investigations into Binance and Zhao's misconduct. Disgorgement and financial penalties between these law enforcement arms in aggregate require Binance to pay more than $4.3 billion.

234. In addition to monetary penalties and forfeiture, Binance's plea agreement requires Binance to be subject to an independent compliance monitor for three years to oversee remediation steps taken to improve Binance's AML program, to admit to a 25-page statement of facts outlining the misconduct, and to cooperate and self-report with respect to any additional violations discovered.

235. Zhao pled guilty to failing to maintain an effective AML program, in violation of federal law. In the plea, Zhao agreed to pay a $150 million fine.

236. Binance entered into an agreement with OFAC to settle charges of violations of multiple sanctions-related regulations, including the Iranian Transactions and Sanctions

Regulations, the Syrian Sanctions Regulations, and Section 594.201(a) of the Global Terrorism Sanctions Regulations, as well as IEEPA.

237. As part of the OFAC settlement, in addition to monetary penalties, Binance agreed to commit to a number of remedial measures to improve its internal controls, audit and training functions and to undertake risk assessments. Binance also agreed to further cooperation with OFAC and to the appointment of a monitor for five years. Binance also agreed to certify annually its efforts to meet the compliance commitments of the agreement.

238. In addition to monetary penalties, Binance agreed to appointment of an independent compliance monitor for a term of five years, to perform a review within 90 days of the monitor's appointment for any U.S. users on the Binance.com platform; to provide a report summarizing the review's findings and offboarded customers within 21 days of completion of the review; and to offboard those users no later than 60 days after providing the report to FinCEN and to certify that those users have been removed. Binance agreed to annual performance of this exercise during the term of the monitorship.

239. Binance also agreed pursuant to the FinCEN settlement to hire a SAR lookback consultant and perform a SAR lookback review of transactions between January 1, 2018 and December 31, 2022 and to report on the findings no later than May 2025, to be followed by the filing of any necessary SARs within 90 days of the report.

240. Binance also agreed to undertake specified measures to improve its AML program and to provide FinCEN with reporting and access to related documentation.

241. OFAC's settlement with Binance is part of a comprehensive settlement with DOJ, FinCEN, and the CFTC, pursuant to which it has undertaken to pay substantial additional penalties and undertake other significant remedial measures.

242. Binance, its Irish affiliates, and Zhao entered into a settlement with the CFTC, admitting various violations of the Commodities Exchange Act and related regulations, including executing futures transactions on an unregistered board of trade, illegally entering into off-exchange options trades, failure to register as a futures commission merchant in violation of; failure to register as a designated contract market or swap execution facility, failure to diligently supervise, including by failing to implement an effective customer identification program, failing to implement effective KYC procedures, failing to implement effective AML procedures, purposefully instructing customers to evade compliance controls and intentionally destroying documents related to illegal conduct, failing to implement a customer identification program, KYC policies and procedures, and AML program, failing to retain required customer information and failure to implement procedures to ascertain whether a customer appears on lists of known or suspected terrorists or terrorist organizations and willful evasion of the Commodities Exchange Act in violation. Zhao's liability was established due to his status as a "control person" of Binance pursuant to 7 U.S.C. § 13c(b).

243. In addition to monetary penalties, Binance was enjoined from continued U.S. operations pertaining to the offering, sale, or execution of digital asset trades in violation of the CEA, to implement an effective AML program, to cease permitting customers to trade through sub-accounts to circumvent compliance controls, to certify compliance, and to create a new board structure that excluded Zhao and included a compliance and audit committee.

244. The CFTC separately entered into a settlement with Binance's former chief compliance officer for aiding and abetting Binance's violations and imposing an injunction and a $1.5 million fine.

245. Hamas and PIJ have long-been designated under U.S. law as FTOs and SDGTs because they murdered hundreds of U.S. and Israeli citizens, acts for which they are globally infamous, and continued to launch attacks against civilians in the years leading up to the attacks. Knowingly providing resources to Hamas and PIJ is to knowingly contribute to foreseeable future attacks on U.S. and Israeli citizens.

246. As a result of decades of legislation by various countries around the world and their creation of highly skilled, dedicated regulatory and law enforcement agencies to monitor terrorism financing, supporters of Hamas and PIJ rightfully encounter numerous obstacles to providing financial support for these terrorist organization. However, when a financial platform or financial institution such as Binance creates a purpose-built freewheeling environment that allows for terrorist supporters to provide financial aid, those supporters will flock to and utilize the platform until it is shut down. Binance allowed, facilitated, and encouraged such funding for many years, providing substantial assistance to the terrorist groups that caused the October 7 Terrorist Attacks.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

AIDING AND ABETTING DESIGNATED FOREIGN TERRORIST ORGANIZATIONS IN VIOLATION OF 18 U.S.C. § 2333(d)(2) (Against Defendants Binance Holdings Limited and Changpeng Zhao)

247. Plaintiffs repeat and reallege each and every allegation of the foregoing paragraphs as if fully set forth herein.

248. Plaintiffs assert this cause of action against Defendants Binance Holdings Limited and Changpeng Zhao under 18 U.S.C. § 2333(d)(2), which provides for liability (in an action under 18 U.S.C. § 2333(a) involving acts of international terrorism by a designated foreign terrorist

organization), against "any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism."

249. Plaintiffs are nationals of the United States who were injured in their persons or property by acts of international terrorism, or the estates, survivors or heirs of such U.S. nationals.

250. Hamas and PIJ were designated FTOs when they committed, planned, and authorized the October 7 Terrorist Attacks that injured and/or killed the Plaintiffs or their family members.

251. The October 7 Terrorist Attacks were acts of international terrorism, as defined by 18 U.S.C. § 2331. The attacks: (a) involved violence and endangered human life; (b) would have violated federal and state criminal law, had they been committed in the United States; (c) appeared to be intended to intimidate or coerce the civilian populations of Israel and the United States, to influence the policies of the Israeli and American governments, and to affect the policies of those governments through violent action; and (d) occurred primarily outside the United States and transcended national boundaries in that Hamas raised money internationally, intended to impact the citizens and governments of Israel and the United States, operated internationally and sought asylum in multiple countries in the Middle East.

252. Defendants Binance Holdings Limited and Changpeng Zhao knowingly provided substantial assistance to Hamas and PIJ.

253. The substantial assistance that Defendants Binance Holdings Limited and Changpeng Zhao knowingly provided to Hamas and PIJ included: (a) transferring significant sums of money to Hamas, PIJ, and their agents; (b) maintaining bank accounts or other financial accounts, or hosting transactions involving cryptocurrency exchange wallets, for the benefit of Hamas, PIJ, their front organizations, and its senior operatives; (c) providing Hamas and PIJ with

access to U.S. dollars and the U.S. banking system; (d) providing seeming legitimacy to Hamas and PIJ's efforts to raise funds to finance its operations and to compensate terrorists and their family members following terrorist attacks; and (e) enabling Hamas and PIJ to access funds that could foreseeably be used to commit terrorist attacks.

254. Specifically, Defendants Binance Holdings Limited and Changpeng Zhao knowingly provided Hamas and PIJ with unrestricted access to Binance's cryptocurrency exchange platform, enabling Hamas and PIJ to receive and send payments, and to engage in cryptocurrency trading for profit, in violation of U.S. law. Such unrestricted access included, but was not limited to: (i) failing to take steps to prevent Hamas and PIJ, designated terrorist organizations, from transacting on Binance's cryptocurrency exchange platform, by either performing no or inadequate customer due diligence, in violation of U.S. law; (ii) concealing the presence of Hamas and PIJ on its cryptocurrency exchange platform, in violation of U.S. law; (iii) facilitating direct transmission of cryptocurrency to and from Hamas and PIJ, in violation of U.S. law; (iv) failing to report known transactions involving Hamas and PIJ, in violation of U.S. law; and (v) permitting Hamas and PIJ to withdraw balances held with Binance.com, in violation of U.S. law. Binance Holdings Limited continued providing these services even after senior executives learned that the platform had provided services to Hamas, PIJ and their funders, despite its knowledge that Hamas and PIJ are terrorist organizations.

255. At the time Defendants Binance Holdings Limited and Changpeng Zhao provided substantial assistance to Hamas and PIJ, they knew that: (a) the U.S. government had designated Hamas and PIJ as FTOs and SDGTS; (b) Hamas and PIJ engaged in acts of international terrorism resulting in the murder of hundreds of Israeli and U.S. citizens; and (c) clandestine funding was essential to Hamas and PIJ's ability to carry out terrorist attacks.

256. Defendants Binance Holdings Limited and Changpeng Zhao also knew that their substantial assistance would facilitate the ability of Hamas and PIJ to carry out terrorist attacks.

257. The assistance that Defendants Binance Holdings Limited and Changpeng Zhao provided to Hamas and PIJ was a substantial factor in causing Plaintiffs' injuries. Moreover, the October 7 Terrorist Attacks, as well as Plaintiffs' injuries in the attacks, were foreseeable results of that substantial assistance.

258. As a direct and proximate result of the substantial, knowing assistance that Defendants Binance Holdings Limited and Changpeng Zhao provided to Hamas and PIJ, Plaintiffs have suffered significant physical, psychological, and emotional injuries.

259. Defendants Binance Holdings Limited and Changpeng Zhao are therefore liable to Plaintiffs for damages in an amount to be determined at trial, treble damages, and the payment of the attorneys' fees and expenses incurred by Plaintiffs in connection with this action.

SECOND CAUSE OF ACTION

PROVIDING MATERIAL SUPPORT TO TERRORISTS IN VIOLATION OF 18 U.S.C §§ 2333(a) AND 2339A (Against Defendants Binance Holdings Limited and Changpeng Zhao)

260. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

261. Plaintiffs assert this claim against Defendants Binance Holdings Limited and Changpeng Zhao for violations of 18 U.S.C. §§ 2333(a) and 2339A. Under 18 U.S.C. § 2333(a), a civil cause of action may be asserted by U.S. nationals who are killed or injured as a result of an "act of international terrorism." The phrase "international terrorism" is defined under 18 U.S.C. § 2331(1) to include, among other things, "violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States." The criminal laws of the United States include

18 U.S.C. § 2339A, which provides for criminal lability for persons who provide material support to terrorists.

262. Plaintiffs are nationals of the United States who were injured in their persons or property by acts of international terrorism, or the estates, survivors or heirs of such U.S. nationals.

263. Defendants Binance Holdings Limited and Changpeng Zhao provided material support to Hamas and PIJ and facilitated their efforts to engage in acts of international terrorism, including the attacks that killed and injured Plaintiffs and their family members.

264. At the time that Defendants Binance Holdings Limited and Changpeng Zhao provided that material assistance to Hamas and PIJ, they knew that Hamas and PIJ were FTOs and SDGTs and that such organizations were transacting on the Binance.com platform. Further, at the time, it was foreseeable to Binance Holdings Limited and Changpeng Zhao that Hamas and PIJ would use that material assistance to prepare for or carry out terrorist attacks. Plaintiffs' injuries were a foreseeable result of the material support and substantial assistance that Defendants provided to Hamas and PIJ.

265. The material assistance that Defendants Binance Holdings Limited and Changpeng Zhao provided to Hamas and PIJ constituted activities dangerous to human life that violated 18 U.S.C. § 2339A and that were either unlawful under state law, including New York Penal Law §§ 490.10 and 490.15, or would have been unlawful under that state law if committed in the United States.

266. The material assistance that Defendants Binance Holdings Limited and Changpeng Zhao provided to Hamas was dangerous to human life because that assistance provided material support to Hamas and PIJ in financing their violent attacks and recruit individuals to carry out those attacks. The financial assistance that Defendants provided to Hamas and PIJ also provided

material support for them to expand their purported charitable activities, and thereby attract additional donors and recruits for terrorist operations.

267. The material assistance that Defendants Binance Holdings Limited and Changpeng Zhao provided to Hamas and PIJ appeared to be intended to (or was made with reckless disregard for the risk that it would): (a) intimidate or coerce the civilian populations of Israel and the United States; (ii) influence the policies of Israel and the United States by means of intimidation and coercion; or (iii) affect the conduct of the governments of Israel and the United States by mass destruction, assassination, or kidnapping.

268. The substantial financial assistance that Defendants Binance Holdings Limited and Changpeng Zhao provided to Hamas and PIJ occurred primarily outside the United States and transcended national boundaries in that Defendants operated internationally in providing financial assistance to Hamas and PIJ.

269. As a result, Defendants Binance Holdings Limited and Changpeng Zhao committed acts of international terrorism, as defined by 18 U.S.C. § 2331.

270. Hamas and PIJ's acts of violence caused the injuries that Plaintiffs suffered and the deaths of Plaintiffs' family members.

271. The material support and substantial assistance that Defendants Binance Holdings Limited and Changpeng Zhao provided to Hamas and PIJ was a substantial factor in causing Plaintiffs' injuries. Moreover, the October 7 Terrorist Attacks, as well as Plaintiffs' injuries in the attacks, were foreseeable results of the material support and substantial assistance that Defendants provided to Hamas and PIJ.

272. As a direct and proximate result of the material support and substantial assistance that Defendants Binance Holdings Limited and Changpeng Zhao knowingly provided to Hamas and PIJ, Plaintiffs have suffered significant physical, psychological, and emotional injuries.

273. Defendants Binance Holdings Limited and Changpeng Zhao are therefore liable to Plaintiffs for damages in an amount to be determined at trial, treble damages, and the payment of the attorneys' fees and expenses incurred by Plaintiffs in connection with this action.

THIRD CAUSE OF ACTION

PROVIDING MATERAL SUPPORT TO FOREIGN TERRORIST ORGANIZATIONS IN VIOLATION OF 18 U.S.C. §§ 2333(a) AND 2339B(a)(1) (Against Binance Holdings Limited and Changpeng Zhao)

274. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

275. Plaintiffs assert this claim against Defendants Binance Holdings Limited and Changpeng Zhao for violation of 18 U.S.C. §§ 2333(a) and 2339B(a)(1). Under 18 U.S.C. § 2333(a), a civil cause of action may be asserted by U.S. nationals who are killed or injured as a result of an "act of international terrorism." The phrase "international terrorism" is defined under 18 U.S.C. § 2331(1) to include, among other things, "violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States." The criminal laws of the United States include 18 U.S.C. § 2339B(a)(1), which provides for criminal lability for persons who provide material support or resources to foreign terrorist organizations.

276. Plaintiffs are nationals of the United States who were injured in their persons or property by acts of international terrorism, or the estates, survivors or heirs of such U.S. nationals.

277. At the time of the attack that injured Plaintiffs, Hamas and PIJ were each an FTO and SDGT.

278. At that time, Defendants Binance Holdings Limited and Changpeng Zhao knew that each of Hamas and PIJ was an FTO and SDGT, that each engaged in terrorist activity (as defined in 8 U.S.C. § 1182(a)(3)(B)), and that each engaged in terrorism (as defined in 22 U.S.C. § 2656f(d)(2)).

279. As Plaintiffs allege in detail above, Defendants Binance Holdings Limited and Changpeng Zhao provided material support to Hamas and PIJ.

280. That material support was integral to the ability of Hamas and PIJ to carry out terrorist attacks, including the attacks that injured Plaintiffs and killed their family members.

281. As Plaintiffs allege in detail above, the material support that Defendants Binance Holdings Limited and Changpeng Zhao provided to Hamas and PIJ constituted acts of international terrorism, as defined in 18 U.S.C. § 2331(1).

282. The material support that Defendants Binance Holdings Limited and Changpeng Zhao provided to Hamas and PIJ was a substantial and foreseeable factor in causing Plaintiffs' injuries.

283. Moreover, the October 7 Terrorist Attacks, as well as Plaintiffs' injuries in the attacks, were foreseeable results of the material support and substantial assistance that Defendants Binance Holdings Limited and Changpeng Zhao provided to Hamas and PIJ.

284. As a direct and proximate result of the material support and substantial assistance that Defendants knowingly provided to Hamas and PIJ, Plaintiffs have suffered significant physical, psychological, and emotional injuries.

285. Defendants Binance Holdings Limited and Changpeng Zhao are therefore liable to Plaintiffs for damages in an amount to be determined at trial, treble damages, and the payment of the attorneys' fees and expenses incurred by Plaintiffs in connection with this action.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that this Court enter judgment against Defendants jointly and severally and in favor of Plaintiffs for:

(a) Compensatory damages in amounts to be determined at trial;

(b) Treble damages pursuant to 18 U.S.C. § 2333(a);

(c) Punitive damages under 28 U.S.C. § 1605A(c);

(d) Any and all costs sustained in connection with the prosecution of this action, including attorneys' fees pursuant to 18 U.S.C. § 2333(a);

(e) Pre-judgment interest; and

(f) Such other and further relief as justice requires.

Dated: May 17, 2024
New York, New York

SEIDEN LAW LLP

/s/ Amiad Kushner

Robert W. Seiden
Amiad Kushner
Jake Nachmani
Jennifer H. Blecher
Dov B. Gold
322 Eighth Ave, Suite 1200
New York, NY 10001
646-766-1914
rseiden@seidenlaw.com
akushner@seidenlaw.com
jnachmani@seidenlaw.com
jblecher@seidenlaw.com
dgold@seidenlaw.com

PERLES LAW FIRM, P.C.

Steven R. Perles (*pro hac vice motion to be filed*)
Joshua K. Perles (*pro hac vice motion to be filed*)
Edward B. MacAllister (*pro hac vice motion to be filed*)
816 Connecticut Avenue, NW
12th Floor
Washington, D.C. 20006
(202) 955-9055

Attorneys for Plaintiffs